Universidade de Aveiro Departamento de Matemática
2008

Sandra Isabel Diogo Ramos

O Monoide Bicíclico: subsemigrupos e generalizações

Universidade de Aveiro Departamento de Matemática
2008

Sandra Isabel Diogo Ramos

O Monoide Bicíclico: subsemigrupos e generalizações

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática (perfil de Ensino), realizada sob a orientação científica do Doutor Luís António Arsénio Descalço e do Doutor Manuel António Gonçalves Martins, Professores Auxiliares do Departamento de Matemática da Universidade de Aveiro.

o júri

presidente

Professora Doutora Maria Paula Macedo Rocha Malonek
Professora Catedrático da Universidade de Aveiro

vogais

Professor Doutor Manuel Augusto Fernandes Delgado
Professor Auxiliar da Universidade do Porto

Professor Doutor Luís António Arsénio Descalço
Professor Auxiliar da Universidade de Aveiro (Orientador)

Professor Doutor Manuel António Gonçalves Martins
Professor Auxiliar da Universidade de Aveiro (Orientador)

agradecimentos

Esta dissertação é dedicada à memória da minha querida mãe em forma de gratidão…

Maria de Lurdes dos Santos Diogo (1955-2006)

palavras-chave Monoide bicíclico, Propriedades, Subsemigrupos, Generalizações.

resumo

Esta dissertação consiste num trabalho de recolha bibliográfica e síntese sobre o monoide bicíclico, B, propriedades, subsemigrupos, e generalizações. Inicia-se o trabalho com uma breve introdução à teoria de semigrupos em geral, com ênfase para os conceitos necessários aos restantes capítulos. Definimos monoide bicíclico e apresentamos algumas propriedades notáveis do mesmo, fazemos a descrição de todos os subsemigrupos de B, que utilizamos para estabelecer diversas propriedades destes subsemigrupos. Estudamos apenas em detalhe uma generalização e referimos outras. Foram incluídos resultados recentes, nomeadamente sobre os subsemigrupos de B.

keywords

Bicyclic Monoid, Properties, Subsemigroups, Generalizations.

abstract

This thesis consists of a work of bibliographical selection and synthesis around the bicyclic monoid, *B*, its properties, subsemigroups, and generalizations. The thesis begins with a brief introduction to the theory of semigroups with emphasis to the required concepts for the remaining chapters. We define the bicyclic monoid and present some of its notable properties. Then we present the description of all the subsemigroups of *B*, which we use to establish several properties of these subsemigroups. We study one generalization in detail and we briefly refer other generalizations. This work includes some recent results, particularly on subsemigroups of *B*.

Conteúdo

Capítulo 1

INTRODUÇÃO E DEFINIÇÕES

Monoide bicíclico $\mathbf{B}$ é definido nesta dissertação pela apresentação $\langle b, c \mid bc = 1\rangle$, considerando $\mathbf{B}$ como sendo o conjunto natural de formas normais $\{c^i b^j : i, j \geq 0\}$, com operação:

$$c^i b^j c^k b^l = \begin{cases} c^{i-j+k} b^l & \text{caso } j \leq k \\ c^i b^{j-k+l} & \text{caso } j > k. \end{cases}$$

O monoide bicíclico é um dos semigrupos mais importantes na teoria de semigrupos. É um dos principais ingredientes das extensões de Bruck-Reilly (ver [18]), é também a base de várias generalizações; ver [1], [4], [11], [17]. O monoide bicíclico é conhecido como tendo propriedades notáveis. Por exemplo, é completamente determinado pelo seu reticulado de subsemigrupos; ver [34] e [35]. Também, como semigrupo inverso, este fica completamente determinado pelo reticulado dos subsemigrupos inversos; ver [8]. Jones [20] estuda semigrupos inversos com a seguinte propriedade: um reticulado de semigrupos contendo todos os idempotentes é distributivo, mostra que o monoide bicíclico é um deles, e descreve o próprio reticulado. Em [27] os autores estudam as propriedades de um subsemigrupo de $\mathbf{B}$ específico. Em [6] e [7] é obtida uma descrição de todos os subsemigrupos do monoide bicíclico que permite demonstrar diversas propriedades dos mesmos.

Neste trabalho começamos por apresentar alguns resultados e definições básicas, no primeiro capítulo; no segundo capítulo descrevemos o monoide bicíclico, propriedades do mesmo e fazemos ainda uma breve referência a algumas das suas aplicações; seguidamente, no terceiro capítulo, fazemos a descrição de todos os subsemigrupos do monoide bicíclico e mostramos que existem essencialmente cinco

diferentes tipos de subsemigrupos; no quarto capítulo, tratamos generalizações do monoide bicíclico, em particular o monoide policíclico e terminamos com algumas considerações finais.

Procura-se que esta dissertação seja auto-contida, incluindo por isso um capítulo com uma breve introdução à teoria de semigrupos em geral, com ênfase para os conceitos necessários aos restantes capítulos. Os resultados fundamentais deste capítulo podem ser encontrados em [18] e [26].

1 Definições básicas

Definição 1.1. Um *grupoide* (S, μ) é constituído por um conjunto S, diferente do vazio, com uma operação binária μ (μ é a aplicação $\mu : S \times S \to S$).

Usaremos a designação *multiplicação* para esta operação binária, e x^n ($n \in \mathbb{N}$), como notação para o produto de n elementos x.

Definição 1.2. O par (S, μ) é um *semigrupo* se a operação μ é *associativa*, isto é, se para todo x, y e z pertencentes a S, se verifica

$$((x, y)\mu, z)\mu = (x, (y, z)\mu)\mu \tag{1.1}$$

(Nesta dissertação, usaremos o símbolo de aplicação à direita.)

A *ordem de um semigrupo* (S, μ) é o cardinal do conjunto subjacente S e denota-se por $|S|$.

Escreveremos simplesmente S em vez de $(S, \bullet)$.

Definição 1.3. Se um semigrupo S verificar a seguinte propriedade,

$$xy = yx \quad \text{para todo } x \text{ e } y \text{ pertencentes a } S$$

dizemos que o semigrupo é *comutativo*.

Definição 1.4. Se existir um elemento 1 pertencente ao semigrupo S que verifica

$$x1 = 1x \quad \text{para todo } x \text{ pertencente a } S$$

dizemos que é um *semigrupo com identidade* ou *monoide*, e dizemos que 1 é a identidade do semigrupo.

Proposição 1.5. *Um semigrupo* S *contém no máximo um elemento identidade.*

DEMONSTRAÇÃO. Suponhamos que existe, em S, um outro elemento identidade e chamemos-lhe $1'$, assim,

$$x1' = 1'x \quad \text{para todo } x \text{ pertencente a } S$$

então,

$$1' = 11' \quad \text{(uma vez que 1 é identidade)}$$

$$1' = 1 \quad \text{(uma vez que } 1' \text{ é identidade).}$$

□

Se o semigrupo S não tem identidade, podemos agregar-lhe o elemento 1, para obter um monoide, definido

$$1s = s1 = s \quad \text{e} \quad 11 = 1 \quad \text{para todo } s \text{ pertencente a } S.$$

Facilmente se verifica que $S \cup \{1\}$ é um monoide.

Definição 1.6. Definimos S^1 como sendo um monoide obtido de S juntando-lhe a identidade, caso seja necessário, isto é,

$$S^1 = \begin{cases} S & \text{caso S tenha identidade} \\ S \cup \{1\} & \text{caso contrário.} \end{cases}$$

Se um semigrupo S, com pelo menos dois elementos, contiver o elemento 0, tal que,

$$0x = x0 = 0 \quad \text{para todo } x \text{ pertencente a } S$$

dizemos que 0 é o *elemento zero de* S (ou simplesmente o *zero*), e que S *é um semigrupo com zero*. Facilmente se verifica que, tal como com o elemento identidade, apenas pode existir um zero em cada semigrupo. A condição de que S tenha pelo menos dois elementos significa que não queremos considerar o semigrupo trivial $\{e\}$ um semigrupo com zero; e é a identidade.

Tal como anteriormente, se S não tem o elemento zero podemos agrelhar-lhe um elemento 0, definindo

$$0x = x0 = 0 \quad \text{para todo } x \text{ pertencente a } S.$$

É trivial verificar que a associatividade ainda se verifica em $S \cup \{0\}$. Analogamente a S^1 definimos S^0:

Definição 1.7. S^0 é um semigrupo obtido de S juntando-lhe o zero, caso seja necessário, isto é,

$$S^0 = \begin{cases} S & \text{caso S tenha identidade} \\ S \cup \{0\} & \text{caso contrário.} \end{cases}$$

Observação 1.8. Embora facilmente se junte um zero ou em elemento identidade a um semigrupo e este se mantenha um semigrupo, não podemos de modo algum restringir o estudo dos semigrupos ao estudo dos monóides com zero, porque, juntando outros elementos a um semigrupo podemos sacrificar algumas propriedades desse semigrupo:

Exemplo 1.9. *Se juntarmos o zero a um semigrupo que seja grupo, obtemos um semigrupo que não é um grupo.*

É trivial verificar que falha a propriedade *existência de elemento inverso*, porque existe um elemento, o zero, que não tem inverso uma vez que, para todo x em S se tem

$$0x = x0 = 0 \neq e \quad \text{(considerando } e \text{ a identidade).}$$

Definição 1.10. Se A e B são subconjuntos de um semigrupo S, então,

$$AB = \{ab : a \in A, b \in B\}.$$

Facilmente se verifica que $(AB)C = A(BC)$.

Note-se que A^2 significa $\{a_1a_2 : a_1, a_2 \in A\}$, e não $\{aa : a \in A\}$. Quando trabalharmos com conjuntos singulares usaremos uma notação simplificada, escrevendo por exemplo Ab em vez de $A\{b\}$.

Se a é um elemento de um semigrupo S sem identidade, então, Sa não contém a necessariamente. Usaremos a seguinte notação

$$\begin{aligned} S^1a &= Sa \bigcup \{a\}, \\ aS^1 &= aS \bigcup \{a\}, \\ S^1aS^1 &= SaS \bigcup Sa \bigcup aS \bigcup \{a\}. \end{aligned} \tag{1.2}$$

Note-se que S^1, aS^1 e S^1aS^1 são subconjuntos de S e não contêm o elemento 1.

Definição 1.11. Se um semigrupo S verificar a seguinte propriedade

$$(\forall a \in S)\ aS = S \text{ e } Sa = S \tag{1.3}$$

dizemos que S é um *grupo*.

Esta não é a definição mais comum de grupo mas facilmente se prova que é equivalente à definição mais usual:

$$\begin{aligned}&(\exists e \in S)(\forall a \in S) \quad ea = a,\\ &(\forall a \in S)(\exists a^{-1} \in S) \quad a^{-1}a = e.\end{aligned} \tag{1.4}$$

A definição de 1.11 é a que aparece mais frequentemente na teoria de semigrupos e é equivalente a

$$(\forall a, b \in S)(\exists x, y \in S) \quad ax = b \text{ e } ya = b \tag{1.5}$$

Se G é um grupo então $G^0 = G \bigcup \{0\}$ é um semigrupo. Este semigrupo chamar-se-á *grupo com zero*, ou um *0-grupo*.

Proposição 1.12. *Um semigrupo com zero é um 0-grupo (grupo com zero) se e só se*

$$(\forall a \in S \backslash \{0\})\ aS = S \ e\ Sa = S.$$

Demonstração. Suponhamos que $S = G^0$ é um $0 - grupo$, e seja $a \in G = S\backslash\{0\}$. É óbvio que $aG = Ga = G$. Uma vez que $aS = aG \bigcup \{0\} = S$ e $Sa = Ga \bigcup \{0\}$ então $aS = Sa = S$. Reciprocamente, suponhamos que S goza da propriedade dada

$$(\forall a \in S \backslash \{0\})\ aS = S \text{ e } Sa = S,$$

e seja $G = S\backslash\{0\}$. Uma vez que S tem mais do que dois elementos temos que $G \neq \varnothing$. Para provar que G é grupo devemos em primeiro lugar mostrar que é fechado para a operação. Suponhamos, por absurdo, que existem a, b em G tais que $ab = 0$. Assim

$$S^2 = (Sa)(bS) = S(ab)S = S0S = \{0\},$$

então $S = aS \subseteq S^2 = \{0\}$, o que é um absurdo. Podemos então concluir que G é fechado para o operação. Desta propriedade sai que para todo a, b em G existem x, y em S tais que $ax = b$ e $ya = b$. Os elementos x e y não podem ser zero, logo estão em G. Assim, G satisfaz (1.5), logo, é um grupo. □

Definição 1.13. Um subconjunto T, diferente do vazio, de S é chamado um *sub-semigrupo* se for fechado para a multiplicação, isto é, verificar a seguinte propriedade

$$(\forall x, y \in T) : xy \in T \tag{1.6}$$

Esta condição pode ser expressa de forma mais compacta por $T^2 \subseteq T$. Como S goza da propriedade associativa e T é um subconjunto de S então, T é também um

semigrupo. Entre os subsemigrupos é de salientar o próprio S, $\{0\}$, $\{1\}$ e também, generalizando $\{e\}$, em que e é qualquer elemento de S que é *idempotente*, isto é, que satisfaz $e^2 = e$.

Definição 1.14. Um subsemigrupo de S que seja um grupo para a multiplicação inerente a S chamar-se-á *subgrupo* de S.

Os subsemigrupos com um só elemento $\{0\}$, $\{1\}$ e $\{e\}$, mencionados no parágrafo anterior, são exemplos triviais disso. Não é difícil ver que qualquer subconjunto T de S é um subgrupo se e só se

$$(\forall a \in T)\ aT = T \ \text{ e } \ Ta = T. \tag{1.7}$$

Definição 1.15. Um subconjunto A, diferente do vazio, de S chama-se *ideal esquerdo* se $SA \subseteq A$, *ideal direito* se $AS \subseteq A$, e simplesmente *ideal* se for, simultaneamente, ideal direito e esquerdo.

É evidente que todo o ideal (quer seja esquerdo, direito ou ideal esquerdo e direito) é um subsemigrupo mas o contrário não se verifica.

Entre os ideais de S é de salientar o próprio S e $\{0\}$ (caso zero seja um elemento de S). Um ideal I tal que $\{0\} \subset I \subset S$ (estritamente) chama-se *ideal próprio*.

Definição 1.16. Uma aplicação $\phi : S \to T$, em que $(S, .)$ e $(T, .)$ são semigrupos é chamado um *morfismo* (ou *homomorfismo*) se, para qualquer x, y em S

$$(xy)\phi = (x\phi)(y\phi).$$

Se $(S, ., 1_S)$ e $(T, ., 1_T)$ forem monóides com os elementos identidade 1_S e 1_T, respectivamente, então ϕ será um morfismo de monoides se verificar adicionalmente a propriedade

$$1_S\phi = 1_T.$$

Há aqui possibilidade de confusão, se surgir alguma dúvida deveremos fazer a distinção entre morfismo de semigrupos e morfismo de monóides.

Definição 1.17. Um morfismo $\phi : S \to T$ é chamado um *isomorfismo* se for invertível, isto é, se existe um morfismo $\phi^{-1} : T \to S$ tal que $\phi\phi^{-1}$ é uma aplicação identidade em S e $\phi^{-1}\phi$ é uma aplicação identidade em T.

Não é difícil mostrar que morfismo $\phi : S \to T$ é um isomorfismo se e só se for bijectivo.

Se $\phi : S \to T$ for isomorfismo, dizemos que S e T são isomorfos e escrevemos $S \backsimeq T$.

Tal como em grupos nos aparecem os grupos de permutações num conjunto, assim nos semigrupos surgem-nos aplicações de um conjunto nele próprio. Há uma analogia entre o semigrupo simétrico $(G_x, \circ)$ de todas as permutações de um conjunto X e o *semigrupo de transformação total* $(T_x, \circ)$ que consiste em todas as aplicações de X em X. A operação em ambos os casos é a composição de aplicações, algumas vezes escrevemos $\circ$, mas frequentemente escrevemos: se α e β são aplicações de X em X, então

$$x(\alpha \circ \beta)(= x(\alpha\beta)) = (x\alpha)\beta \quad (x \in X).$$

É claro que G_x, que consiste em todas as bijecções de X em X, é um subsemigrupo de T_x.

Se um semigrupo S é, para algum X, um subsemigrupo de T_x dizemos que S é um *semigrupo de aplicações*, ou *semigrupo de transformações.* Um morfismo ϕ de um semigrupo S em algum T_x é chamada uma *representação de* S, e ϕ é chamada *representação fiel* se for injectiva.

O teorema seguinte, muito "próximo"do teorema de Cayley para grupos, mostra que cada semigrupo é isomorfo a um semigrupo de transformações:

Teorema 1.18. *Se S é um semigrupo e $X = S^1$ então existe uma representação fiel $\phi : S \to \mathcal{T}_X$.*

Demonstração. Para cada $a \in S$, defina-se a aplicação $\rho_a : S^1 \to S^1$ do seguinte modo

$$x\rho_a = xa \quad (x \in S^1).$$

Deste modo $\rho_a \in \mathcal{T}_X$ (porque é uma aplicação de S^1 em S^1), e portanto existe a aplicação $\alpha : S \to \mathcal{T}_X$ definida por

$$a\alpha = \rho_a \quad (a \in S).$$

A aplicação é injectiva, uma vez que quaisquer que sejam a, b pertencentes a S,

$$a\alpha = b\alpha \Rightarrow \rho_a = \rho_b \Rightarrow xa = xb \quad (\forall a \in S^1)$$

$$\Rightarrow 1a = 1b \Rightarrow a = b.$$

Note-se que isto não seria válido se tivéssemos considerado S em vez de S^1.

Uma vez que, para todo o x pertencente a S^1 se tem

$$x(\rho_a\rho_b) = (x\rho_a)\rho_b = (xa)b = x(ab) = x\rho_{ab},$$

temos $(a\alpha)(b\alpha) = (ab)\alpha$. □

A representação α que nos aparece na demonstração anterior é chamada *representação regular direita extendida* de S. A palavra "extendida" aqui significa que S^1 é usado como sendo o conjunto X.

2 Semigrupos monogénicos

Seja S um semigrupo, e seja $\{U_i : i \in I\}$ (com $I \neq \varnothing$) uma família indexada de subsemigrupos de S. Facilmente se verifica que a intersecção U de todos subsemigrupos U_i, se não for vazia, é ainda um subsemigrupo de S. Para cada subconjunto A de S, não vazio, existe pelo menos um subsemigrupo de S que contém o A, nomeadamente o próprio S. Por esta razão a intersecção de todos os subsemigrupos de S que contém A é um subsemigrupo de S que contém A, que denotaremos por $\langle A\rangle$. Note-se que $\langle A\rangle$ é subsemigrupo definido pelas seguintes propriedades

(1) $A \subseteq \langle A\rangle$;

(2) Se U é um subsemigrupo de S que contém A, então $\langle A\rangle \subseteq U$.

O subsemigrupo $\langle A\rangle$ consiste em todos os elementos de S que podem ser expressos como um número finito de produtos de elementos de A. Se $\langle A\rangle = S$ dizemos que A é um conjunto gerador de S.

É particularmente interessante o caso em que A é finito. Se $A = \{a_1, a_2, ..., a_n\}$ então escrevemos $\langle A\rangle$ como $\langle a_1, a_2, ..., a_n\rangle$. No caso em que $A = \{a\}$, um conjunto singular, temos

$$\langle a\rangle = \{a, a^2, a^3, ...\}.$$

Neste ponto vale a pena notar que se S é um monoide podemos do mesmo modo falar em *submonoide* de S gerado por A, que conterá sempre o 1. No caso de um conjunto singular temos

$$\langle a\rangle = \{1, a, a^2, a^3, ...\}.$$

Referimo-nos a $\langle a\rangle$ como sendo um *subsemigrupo monogénico* gerado pelo elemento a. A *ordem* do elemento a é definida, tal como em teoria de grupos, como sendo a ordem do semigrupo $\langle a\rangle$. Se S é um semigrupo onde existe um elemento a tal que $S = \langle a\rangle$, então S é chamado um *semigrupo monogénico*.

Seja a um elemento de um semigrupo S, e considere-se o subsemigrupo monogénico

$$\langle a\rangle = \{a, a^2, a^3, ...\}$$

gerado por a. Se não houver repetições em $a, a^2, a^3, ...$, isto é, se

$$a^m = a^n \Rightarrow m = n$$

então, é evidente que $(\langle A\rangle, \cdot)$ é isomorfo ao semigrupo $(\mathbb{N}, +)$, dos números naturais com a adição usual. Neste caso, dizemos que a é um *semigrupo monogénico infinito*, e que a tem ordem infinita em S.

Suponhamos agora que existem repetições entre as potências de a. Então o conjunto

$$\{x \in \mathbb{N},\ (\exists y \in \mathbb{N})\ a^x = a^y,\ x \neq y\}$$

é não vazio e tem um elemento mínimo. Denotemos esse elemento por m e chamemos-lhe *índice* do elemento a. Então o conjunto

$$\{x \in \mathbb{N} : a^{m+x} = a^m\}$$

é não vazio e tem também um elemento mínimo r, que chamaremos o período de a. Referir-nos-emos a m e a r como índice e período, respectivamente, do semigrupo monogénico $\langle a\rangle$.

Seja a um elemento com índice m e período r. Assim,

$$a^m = a^{m+x} \tag{1.8}$$

e por conseguinte

$$a^m = a^{m+r} = a^m \cdot a^r = a^{m+r}a^r = a^{m+2r}.$$

Generalizando,

$$\forall q \in \mathbb{N} : a^m = a^{m+qr}.$$

Pela minimalidade de m e r, em (1.8), podemos deduzir que se potências

$$a, a^2, ..., a^m, a^{m+1}, ..., a^{m+r-1}$$

são todas distintas. Para todo $s \geq m$ podemos, pelo algoritmo da divisão, escrever $s = m + qr + u$, em que $q \geq 0$ e $0 \leq r - 1$. Daqui sai que

$$a^s = a^{m+qr}a^u = a^m a^u = a^{m+u};$$

assim,

$$\langle a\rangle = \{a, a^2, ..., a^{m+r-1}\}, \qquad \text{e} \qquad |\langle A\rangle| = m + r - 1.$$

Dizemos que a tem *ordem finita*; a ordem é dada pela seguinte regra

$$(\text{ordem de a}) = (\text{índice de a}) + (\text{período de a}) - 1$$

O subconjunto $K_a = \{a^m, a^m + 1, ..., a^{m+r-1}\}$ de $\langle a \rangle$ é um subsemigrupo e um ideal de $\langle a \rangle$. Chamamos-lhe *Kernel* de $\langle a \rangle$.

Na verdade, K_a é um grupo cíclico. Para confirmar isto, note-se que os inteiros

$$m, m + 1, ..., m + r - 1$$

formam um conjunto completo de resíduos incongruentes modulo r. Portanto, existe g tal que

$$0 \leq g \leq r - 1, \qquad \text{e} \qquad m + g \equiv 1(\text{mod } r). \tag{1.9}$$

Por isso, $k(m + g) \equiv k \text{ mod } r$, para todo o k pertencente a $\mathbb{N}$, e assim a potência $(a^{m+g})^k$ de (a^{m+g}), para $k = 1, 2, ..., r$, cobre K_a. Deste modo, K_a é um grupo cíclico de ordem r, gerado por (a^{m+g}).

Se escolhermos z de tal modo que

$$0 \leq z \leq r - 1 \qquad \text{e} \qquad m + z \equiv 0(\text{mod } r) \tag{1.10}$$

então a^{m+z} é *idempotente*, e portanto é a identidade de K_a.

Teorema 1.19. *Seja a um elemento de um semigrupo S. Então, ou se verifica*

(1) *todas potências de a são distintas, e o subsemigrupo monogénico $\langle a \rangle$ de S é isomorfo ao semigrupo $(\mathbb{N}, +)$, de números naturais com a adição; ou*

(2) *existem inteiros positivos m (o índice de a) e r (o período de a) que verificam as seguintes propriedades:*

   (a) $a^m = a^{m+r}$;

   (b) *para todo u, v pertencentes a* $\mathbb{N}^0$, $a^{m+u} = a^{m+v}$ *se e só se* $u \equiv v(mod r)$;

   (c) $\langle a \rangle = \{a, a^2, ..., a^{m+r-1}\}$;

   (d) $K_a = \{a^m, a^{m+1}, ..., a^{m+r-1}\}$ *é um subgrupo cíclico de* $\langle a \rangle$.

□

Um semigrupo diz-se *periódico* se todos os seus elementos têm ordem finita. Assim, um semigrupo finito tem necessariamente ordem finita.

Proposição 1.20. *Num semigrupo periódico todos os elementos têm uma potência que é idempotente, isto é, um semigrupo periódico tem, pelo menos, um idempotente.*

DEMONSTRAÇÃO. Se $a \in S$, semigrupo periódico, então $\langle a \rangle$ é finito, logo a^n, para algum $n \in \mathbb{N}$ é a identidade do grupo K_a. □

3 Conjuntos ordenados, semireticulados e reticulados

Definição 1.21. Uma relação binária w num conjunto X (isto é, num subconjunto w de $X \times X$) diz-se uma *ordem* (parcial) se

(O_1) $(x, x) \in w$ para todo x pertencente a X - isto é, w é *reflexiva*;

(O_2) $(\forall x, y \in X)(x, y) \in w$ e $(x, y) \in w \Rightarrow x = y$ - isto é, w é *anti-simétrica*;

(O_3) $(\forall x, y, z \in X)(x, y) \in w$ e $(y, z) \in w \Rightarrow (x, z) \in w$ - isto é, w é *transitiva*.

O par $(X, \leq)$ em que X é um conjunto e $\leq$ é uma ordem parcial, diz-se um *conjunto parcialmente ordenado* (*poset*).

Usaremos $x \leq y$ em vez de $(x, y) \in w$, e também $x \geq y$, $x < y$ e $x > y$ que significa $(y, x) \in w$, $(x, y) \in w$ e $x \neq y$, e $(y, x) \in w$ e $x \neq y$, respectivamente.

Uma ordem parcial que goze da seguinte propriedade

(O_4) $(\forall x, y \in X) \qquad x \leq y$ ou $y \leq x$

diz-se uma *ordem total*.

Seja Y um subconjunto, não vazio, de um conjunto parcialmente ordenado $(X, \leq)$. Um elemento a de Y é *minimal* se não existe um elemento de Y que seja estritamente inferior a a, isto é, se

$$(\forall y \in Y) \;\; y \leq a \Rightarrow y = a.$$

Um elemento b de Y é *mínimo* se

$$(\forall y \in Y) \;\; b \leq y.$$

É óbvio que um elemento mínimo é minimal, mas num conjunto parcialmente ordenado é perfeitamente possível termos elementos minimais que não são mínimos.

Proposição 1.22. *Seja Y um subconjunto, não vazio, de um conjunto parcialmente ordenado X. Então*

(1) *Y tem no máximo um elemento mínimo ;*

(2) *Se Y for totalmente ordenado, então os termos "minimal"e "mínimo"são equivalentes.*

□

Dizemos que $(X, \leq)$ satisfaz a condição de minimalidade se todo conjunto X, diferente do vazio, tem um elemento mínimo. Um conjunto X totalmente ordenado satisfazendo a condição de minimalidade diz-se bem ordenado.

Se Y for um subconjunto de $(X, \leq)$, diferente do vazio, dizemos que um elemento c de X é um limite inferior de Y se $c \leq y$ para todo y pertencente a Y. Se o conjunto dos limites inferiores de Y for não vazio e tem um elemento máximo d, dizemos que d é o *maior limite inferior* de Y. O elemento d, caso exista é único; escrevemos

$$d = \bigwedge \{y : y \in Y\}.$$

Se $Y = \{a, b\}$ então escrevemos $d = a \wedge b$.

Se $(X, \leq)$ for tal que existe $a \wedge b$ para todo a, b pertencente a X, então dizemos que $(X, \leq)$ é um *semireticulado inferior*. Se se verificar a propriedade mais forte de tal modo que existe $\bigwedge \{y : y \in Y\}$, para todo subconjunto Y de X, então dizemos $(X, \leq)$ é um *semireticulado inferior completo*. Num semireticulado inferior $(X, \leq)$ temos que, para todo a, b pertencente a X,

$$a \leq b \text{ se e só se } a \wedge b = a. \tag{1.11}$$

Definições análogas são dadas para *menor limite superior*,

$$\bigvee \{y : y \in Y\},$$

para $a \vee b$, para um *semireticulado superior* e para *semireticulado superior completo*.

Se $(X, \leq)$ for simultaneamente um semireticulado superior (completo) e um semireticulado inferior (completo) chamamos-lhe um *reticulado* (*completo*). Nestas circunstâncias podemos querer enfatizar a estrutura de reticulado escrevendo $X = (X, \leq, \wedge, \vee)$. Um *subreticulado* de X é um subconjunto, diferente do vazio, Y de X tal que

$$a, b \in Y \Rightarrow a \wedge b,\ a \vee b \in Y.$$

Seja $(E, \leq)$ um semireticulado inferior. Então, verifica-se, para a, b e c pertencentes a E, que tanto $(a \wedge b) \wedge c$ como $a \wedge (b \wedge c)$ são os maiores limites inferiores

de $\{a, b, c\}$, e deduzimos que

$$(a \wedge b) \wedge c = a \wedge (b \wedge c).$$

Assim $(E, \wedge)$ é um semigrupo. Como $a \wedge a = a$ para todo a pertencente a E e $a \wedge b = a \wedge a$ para todo a, b pertencentes a E, pela formula 1.11, provamos metade da proposição seguinte:

Proposição 1.23. *Seja $(E, \leq)$ um semireticulado inferior. Então $(E, \wedge)$ é um semigrupo comutativo composto inteiramente de idempotentes, e*

$$(\forall a, b \in E)\ a \leq b \ \text{ se e só se } \ a \wedge b = a. \tag{1.12}$$

Reciprocamente, suponhamos que $(E, .)$ é um semigrupo de idempotentes comutativo. Então, a relação $\leq$ em E definida por

$$a \leq b \ \text{ se e só se } \ ab = a$$

é uma ordem parcial em E, relativamente à qual $(E, \leq)$ é um semireticulado inferior. Em $(E, \leq)$ o maior limite inferior de a e b é o seu produto ab.

Demonstração. Seja $(E, .)$ um semigrupo de idempotentes comutativo, e seja $\leq$ definido por 1.12. Uma vez que $a^2 = a$ então $a \leq a$ para todo a pertencente a E. Suponhamos agora que $a \leq b$ e $b \leq a$; então $ab = a$ e $ba = b$ e portanto

$$a = ab = ba = b.$$

Suponhamos seguidamente que $a \leq b$ e $b \leq c$; então $ab = a$ e $bc = b$ e portanto

$$ac = (ab)c = a(bc) = ab = a,$$

e portanto $a \leq c$. Provamos assim que $\leq$ é uma ordem parcial.

Como $a(ab) = a^2b = ab$ e $b(ab) = ab^2 = ab$ temos $ab \leq a$, $ab \leq b$. Se $c \leq a$ e $c \leq b$ então

$$c(ab) = (ca)b = cb = c,$$

e portanto $c \leq ab$. Logo, ab é o único maior limite inferior de a e b. □

A consequência desta proposição é que as noções de "semireticulado inferior" e "semigrupo de idempotentes comutativo" são equivalentes e permutáveis. Usaremos o termo "semireticulado" em qualquer dos dois casos.

O seguinte conceito também vai ser necessário. Seja $(X, \leq)$ um conjunto parcialmente ordenado. Um subconjunto Y de X diz-se um *ideal ordenado* se $x \leq y$ e $y \in Y$ implica que $x \in Y$. O mais pequeno *ideal principal ordenado* de X contendo um elemento x é o conjunto $[x] = \{y \in Y : \ y \leq x\}$. Em geral, se A é um qualquer subconjunto de X então

$$[A] = \{y \in X : \ y \leq a \text{ para algum } a \in A\}$$

é o *ideal ordenado gerado por A*.

4 Relações binárias; equivalências

Sobre conjuntos ordenados devemos ficar com a ideia de que *relação (binária)* num conjunto X é, simplesmente, um subconjunto do produto cartesiano $(X \times X)$.

Intuitivamente podemos pensar nos elementos x e y como estando *relacionados*, e frequentemente escrevemos $x\rho y$ em vez de $(x, y) \in \rho$. O subconjunto vazio $\emptyset$ de $(X \times X)$ está incluído nas relações binárias em X; outras das relações que merecem destaque é a *relação universal* $(X \times X)$, em tudo está relacionado com tudo o resto, e a *relação igualdade*

$$1_x = \{(x, x) : x \in X\},$$

também conhecida como *relação diagonal*, em que dois elementos estão relacionados se e só se forem iguais.

Denotemos por $\mathcal{B}_x$ ao conjunto de todas as relações binárias em X. Uma operação binária $\circ$ é definida em $\mathcal{B}_x$ da seguinte forma: para todo ρ, σ em $\mathcal{B}_x$,

$$\rho \circ \sigma = (x, y) \in X \times X : (\exists z \in X)(x, z) \in \rho \quad \text{e} \quad (x, y) \in \sigma.$$

Neste momento definimos *equivalência* ρ num conjunto X:

Definição 1.24. Uma relação de *equivalência* é uma relação que é reflexiva, simétrica e transitiva, isto é

(E_1) $(x, x) \in \rho$ para todo x pertencente a X - isto é ρ é *reflexiva*;

(E_2) $(\forall x, y \in X)(x, y) \in \rho \Rightarrow (y, x) \in \rho$ - isto é, ρ é *simétrica*;

(E_3) $(\forall x, y, z \in X)(x, y) \in \rho$ e $(y, z) \in \rho \Rightarrow (x, z) \in \rho$ - isto é, ρ é *transitiva*.

Definição 1.25. Uma família de subconjuntos, $\pi = \{A_i : i \in I\}$, de um conjunto X diz-se uma *partição* de X se

(P_1) Cada A_i é não vazio;

(P_2) Para todo i, j em I, ou $A_i = A_j$ ou $A_i \bigcap A_j = \emptyset$;

(P_3) $\bigcup\{A_i : i \in I\} = X$.

As noções de "partição"e "equivalência"são bastante diferentes, mas na verdade estão fortemente relacionadas.

Proposição 1.26. *Seja ρ uma equivalência no conjunto X. Então a família*

$$\Phi(\rho) = \{x\rho : x \in X\}$$

de subconjuntos de X é uma partição de X.

Reciprocamente, se $\pi = \{A_i : i \in I\}$ é uma partição de X, então a relação

$$\Psi(\pi) = \{(x, y) \in X \times X : (\exists i \in I)x, y \in A_i\}$$

é uma equivalência em X.

Para cada equivalência ρ em X, $\Psi(\Phi(\rho)) = \rho$, e para cada partição π de X, $\Phi(\Psi(\pi)) = \pi$.

□

Se ρ é uma equivalência em X, escrevemos algumas vezes $x\rho y$ ou $x \equiv y(mod\rho)$ como alternativa a $(x, y) \in \rho$. Os conjuntos $x\rho$ que formam uma partição associada à equivalência são chamados $classes - \rho$ ou *classes de equivalência*. O conjunto $classes - \rho$, cujos elementos são os subconjuntos $x\rho$, é chamado o conjunto quociente de X por ρ e escrevemos X/ρ. Na próxima secção teremos oportunidade de examinar a aplicação natural $\rho^\natural$ (lê-se "ρ natural") entre X e X/ρ definida do seguinte modo:

$$x\rho^\natural = x\rho \qquad (x \in X) \tag{1.13}$$

Uma importante ligação entre aplicações e equivalências é dada por

Proposição 1.27. *Se $\phi : X \to Y$ é uma aplicação então $\phi \circ \phi^{-1}$ é uma equivalência.*

Demonstração. A forma mais fácil de provar é ver que

$$\begin{aligned} \phi \circ \phi^{-1} &= \{(x, y) \in X \times X : (\exists z \in X)(x, z) \in \phi, (y, z) \in \phi\} \\ &= \{(x, y) \in X \times X : x\phi = y\phi\}. \end{aligned}$$

É claro que $\phi \circ \phi^{-1}$ é reflexiva, simétrica e transitiva.

□

Chamamos à equivalência $\phi \circ \phi^{-1}$ o *kernel* de ϕ, e escrevemos $\phi \circ \phi^{-1} = ker\phi$. Note-se que $ker\rho^\natural = \rho$

Se $\mathbf{R}$ é uma qualquer relação em X, então a família de equivalências que contém $\mathbf{R}$ é não vazia; por esta razão a intersecção de todas as equivalências que contém $\mathbf{R}$ é ainda uma equivalência, a única equivalência mínima em X que contém $\mathbf{R}$. Chamamos-lhe a equivalência *gerada por* $\mathbf{R}$, e denotamos por $\mathbf{R}^e$.

Seja $\mathbf{S}$ uma relação em X, tal que $1_X \subseteq \mathbf{S}$, uma relação que na verdade é reflexiva. Assim temos,

$$\mathbf{S} \subseteq \mathbf{S} \circ \mathbf{S} \subseteq \mathbf{S} \circ \mathbf{S} \circ \mathbf{S} \subseteq ...,$$

que é o mesmo que

$$\mathbf{S} \subseteq \mathbf{S}^2 \subseteq \mathbf{S}^3 \subseteq ...$$

A relação

$$\mathbf{S}^\infty = \bigcup \{\mathbf{S}^n : n \geq 1\} \tag{1.14}$$

é chamado *fecho transitivo* da relação de $\mathbf{S}$.

Lema 1.28. *Para toda a relação reflexiva $\boldsymbol{S}$ num conjunto X, a relação $\boldsymbol{S}^\infty$ definida em (1.14) é a mais pequena relação transitiva em X que contém $\boldsymbol{S}$.*

Demonstração. Primeiro, provemos que $\mathbf{S}^\infty$ é transitiva. Suponhamos que $(x, y), (y, z) \in \mathbf{S}^\infty$. Então existe m e n, dois inteiros positivos, tais que $(x, y) \in \mathbf{S}^m$ e $(y, z) \in \mathbf{S}^n$. Assim,

$$(x, z) \in \mathbf{S}^m \circ \mathbf{S}^n = \mathbf{S}^{m+n} \subseteq \mathbf{S}^\infty.$$

É claro que $\mathbf{S}^\infty$ contém $\mathbf{S}^1 = \mathbf{S}$.

E por fim, se $\mathbf{T}$ é uma relação transitiva que contém $\mathbf{S}$, então

$$\mathbf{S}^2 = \mathbf{S} \circ \mathbf{S} \subseteq \mathbf{T} \circ \mathbf{T} \subseteq \mathbf{T},$$

generalizando, $\mathbf{S}^n \subseteq \mathbf{T}$ para todo $n \geq 1$. Logo, $\mathbf{S}^\infty \subseteq \mathbf{T}$. □

Proposição 1.29. *Para cada relação $\boldsymbol{R}$ no conjunto X,*

$$\boldsymbol{R}^e = [\boldsymbol{R} \cup \boldsymbol{R}^{-1} \cup 1_X]^\infty.$$

Demonstração. Do lema anterior sabemos que a relação $\mathbf{E} = [\mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X]^\infty$ é transitiva e contém $\mathbf{R}$. Uma vez que

$$1_X \subseteq \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X \subseteq \mathbf{E},$$

$\mathbf{E}$ é também reflexiva. É certo que a relação $S = \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X$ é simétrica, daqui vem, para todo n pertencente a $\mathbb{N}$,

$$S^n = (S^{-1})^n = (S^n)^{-1},$$

Assim $\mathbf{S}^n$ é simétrica. Logo $\mathbf{E} = \mathbf{S}^\infty$ é simétrica, uma vez que

$$\begin{aligned}(x,y) \in \mathbf{E} &\Rightarrow (\exists n \in \mathbb{N})(x,y) \in \mathbf{S}^n \\ &\Rightarrow (\exists n \in \mathbb{N})(y,x) \in \mathbf{S}^n \\ &\Rightarrow (y,x) \in \mathbf{E}.\end{aligned}$$

Mostramos que $\mathbf{E}$ é uma relação de equivalência que contém $\mathbf{R}$.

Suponhamos agora que σ é uma relação de equivalência que contém $\mathbf{R}$. Então $1_X \subseteq \sigma$, e $\mathbf{R}^{-1} \subseteq \sigma^{-1} = \sigma$. Logo,

$$\mathbf{S} = \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X \subseteq \sigma.$$

Além disso,

$$\mathbf{S} \circ \mathbf{S} \subseteq \sigma \circ \sigma = \sigma,$$

generalizando, $\mathbf{S}^n \subseteq \sigma$ para todo $n \geq 1$. Daqui sai que $\mathbf{E} = \mathbf{S}^\infty \subseteq \sigma$. Mostramos que $\mathbf{E} = \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X$ é a mais pequena equivalência em X que contém $\mathbf{R}$. Assim,

$$\mathbf{R}^e = [\mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X]^\infty,$$

como pretendíamos demonstrar.

□

5 Congruências

Seja S um semigrupo. Uma relação $\mathbf{R}$ no conjunto S chama-se *compatível à esquerda* (com a operação em S) se

$$(\forall s,t,a \in S) \qquad (s,t) \in \mathbf{R} \Rightarrow (as,at) \in \mathbf{R},$$

e *compatível à direita* se

$$(\forall s,t,a \in S) \qquad (s,t) \in \mathbf{R} \Rightarrow (sa,ta) \in \mathbf{R}.$$

Chama-se *compatível* se

$$(\forall s,t,s',t' \in S) \qquad [(s,t) \in \mathbf{R} \text{ e } (s',t') \in \mathbf{R}] \Rightarrow (ss',tt') \in \mathbf{R}.$$

Uma equivalência que seja compatível à esquerda [direita] é chamada uma *congruência à esquerda* [direita]. Uma relação de equivalência compatível é uma ***congruência***.

Proposição 1.30. *Uma relação ρ num semigrupo S é uma congruência se e só se é simultaneamente uma congruência à direita e à esquerda.*

DEMONSTRAÇÃO. Suponhamos que ρ é uma congruência. Se $(s,t) \in \rho$ e $a \in S$ então $(a,a) \in \rho$ pela reflexividade, e ainda $(as,at) \in \rho$ e $(sa,ta) \in \rho$ pela compatibilidade. Assim, ρ é compatível à direita e à esquerda.

Reciprocamente, suponhamos que ρ é uma congruência à direita e à esquerda, e seja $(s,t),(s',t') \in \rho$. Como ρ é compatível à direita $(ss',ts') \in \rho$, como ρ é compatível à esquerda $(ts',tt') \in \rho$. Podemos concluir por transitividade que $(ss',tt') \in \rho$. Logo, ρ é uma congruência. □

Definição 1.31. Se ρ é uma congruência num semigrupo S então podemos definir uma operação binária no conjunto quociente S/ρ do seguinte modo

$$(a\rho)(b\rho) = (ab)\rho \tag{1.15}$$

A operação está bem definida, precisamente porque ρ é compatível: para todo a,a',b,b' em S,

$$\begin{aligned} a\rho = a'\rho \text{ e } b\rho = b'\rho &\Rightarrow (a,a') \in \rho \text{ e } (b,b') \in \rho \\ &\Rightarrow (ab,a'b') \in \rho \\ &\Rightarrow (ab)\rho = (a'b')\rho. \end{aligned}$$

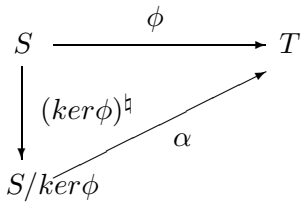
Facilmente se verifica que esta operação é associativa, e portanto, S/ρ é um semigrupo.

Teorema 1.32. *Seja S um semigrupo, e seja ρ uma congruência em S. Então S/ρ é um semigrupo, com a operação definida em (1.15) e a aplicação $\rho^\natural$ de S em S/ρ dada por (1.13) é um morfismo.*

Seja T um semigrupo e seja $\phi : S \to T$ um morfismo. Então a relação

$$ker\phi = \phi \circ \phi^{-1} = \{(a,b) \in S \times S : a\phi = b\phi\}$$

é uma congruência em S, e existe um monomorfismo $\alpha : S/ker\phi \to T$ tal que $im\alpha = im\phi$ e o diagrama



é comutativo.

DEMONSTRAÇÃO. Facilmente se verifica que $\rho^\natural$ é um morfismo.

Para a segunda parte do teorema, supomos que $\phi : S \to T$ é um morfismo. Da proposição (1.27) tiramos que $ker\phi$ é uma equivalência. Para mostrar que é uma congruência, supomos que $(a, a'), (b, b') \in ker\phi$. Então $a\phi = a'\phi$ e $b\phi = b'\phi$, daqui podemos deduzir que

$$(ab)\phi = (a\phi)(b\phi) = (a'\phi)(b'\phi) = (a'b')\phi.$$

assim, $(ab, a'b') \in ker\phi$, tal como pretendido. Para simplificar, denotemos $ker\phi$ por K e definimos $\alpha : S/k \to T$ por

$$(ak)\alpha = a\phi \qquad (a \in S).$$

Então, α está bem definido e é injectiva, uma vez que

$$ak = bk \Leftrightarrow (a, b) \in k \Leftrightarrow a\phi = b\phi.$$

É também um morfismo, uma vez que, para todo a, b pertencentes a S se tem

$$\begin{aligned}[(ak)(bk)]\alpha &= [(ab)k]\alpha = (ab)\phi \\ &= (a\phi)(b\phi) = [(ak)\alpha][(bk)\alpha].\end{aligned}$$

Claramente $im\alpha = im\phi$, e da definição de α é também claro que, para todo a pertencente a S,

$$ak^\natural\alpha = a\phi.$$

□

Para uma qualquer relação $\mathbf{R}$ em S definimos

$$\mathbf{R}^c = \{(xay, xby) : x, y \in S^1, (a, b) \in \mathbf{R}\}.$$

Então,

Lema 1.33. *$\boldsymbol{R}^c$ é a mais pequena relação compatível à direita e à esquerda que contém $\boldsymbol{R}$.*

DEMONSTRAÇÃO. Primeiro, é claro que $\mathbf{R}^c$ contém $\mathbf{R}$. Para mostrar que $\mathbf{R}^c$ é compatível à esquerda, supomos que $(u, v) \in \mathbf{R}^c$ e $w \in S$. Então, $u = xay$, $v = xby$ para algum x, y pertencentes a S^1 e algum (a, b) pertencentes a $\mathbf{R}$. Assim $wu = (wx)ay$ e $wv = (wx)by$, e portanto $(wu, wv) \in \mathbf{R}^c$ como pretendido. A compatibilidade à direita prova-se de forma análoga.

Suponhamos agora que $\mathbf{S}$ é uma relação compatível à direita e à esquerda que contém $\mathbf{R}$. Então, para todo x, y pertencentes a S^1 e para todo (a, b) pertencente a $\mathbf{R}$ temos que $(xay, xby) \in \mathbf{S}$. Logo, $\mathbf{R}^c \subseteq \mathbf{S}$, tal como pretendido. □

Vejamos agora algumas propriedades de $\mathbf{R}^c$:

Lema 1.34. *Sejam $\boldsymbol{R}$, $\boldsymbol{S}$ relações no semigrupo S. Então:*

(1) $\boldsymbol{R} \subseteq \boldsymbol{S} \Rightarrow \boldsymbol{R}^c \subseteq \boldsymbol{S}^c$;

(2) $(\boldsymbol{R}^{-1})^c = (\boldsymbol{R}^c)^{-1}$;

(3) $(\boldsymbol{R} \cup \boldsymbol{S})^c = \boldsymbol{R}^c \cup \boldsymbol{S}^c$.

Seguidamente temos,

Lema 1.35. *Seja $\boldsymbol{R}$ uma relação compatível à direita e à esquerda num semigrupo S. Então $\boldsymbol{R}^n (= \boldsymbol{R} \circ \boldsymbol{R} \circ ... \circ \boldsymbol{R})$ é compatível à direita e à esquerda para todo $n \geq 1$.*

DEMONSTRAÇÃO. Seja $(s, t) \in \mathbf{R}$. Então, existem $z_1, z_2, ..., z_{n-1}$ pertencentes a S tais que

$$(s, z_1), (z_1, z_2), ..., (z_{n-1}, t) \in \mathbf{R}.$$

Sabendo que $\mathbf{R}$ é compatível à direita e à esquerda, temos que, para todo a pertencente a S,

$$(as, az_1), (az_1, az_2), ..., (az_{n-1}, at) \in \mathbf{R},$$

$$(sa, z_1a), (z_1a, z_2a), ..., (z_{n-1}a, ta) \in \mathbf{R}.$$

Logo, $(as, at), (sa, ta) \in \mathbf{R}^n$. □

Seguidamente caracterizaremos $\mathbf{R}^\#$, a congruência em S gerada por $\mathbf{R}$:

Proposição 1.36. *Para cada relação $\boldsymbol{R}$ num semigrupo S, $\boldsymbol{R}^\# = (\boldsymbol{R}^c)^e$.*

DEMONSTRAÇÃO. Da proposição 1.29, sabemos que $(\mathbf{R}^c)^e$ é uma relação de equivalência que contém $(\mathbf{R}^c)$, e portanto contém $\mathbf{R}$. Para mostrar que $(\mathbf{R}^c)^e$ é uma congruência, temos que mostrar que é compatível tanto à direita como è esquerda. Suponhamos que $(s,t) \in (\mathbf{R}^c)^e$ e $a \in S$. Então pela proposição 1.29, $(s,t) \in \mathbf{S}^n$ para algum n pertencente a $\mathbb{N}$, em que $\mathbf{S} = \mathbf{R}^c \cup (\mathbf{R}^c)^{-1} \cup 1_S^c$. Agora, pelo lema 1.34, e pelo facto de que $1_S^c = 1_S$,

$$\mathbf{S} = \mathbf{R}^c \cup (\mathbf{R}^{-1})^c \cup 1_S^c = (\mathbf{R} \cup \mathbf{R}^{-1} \cup 1_S)^c.$$

Logo, $\mathbf{S}$ é compatível à esquerda e à direita pelo lema 1.33, e assim, pelo lema 1.35, também $\mathbf{S}^n$ o é. Daqui sai que

$$(as, at) \in \mathbf{S}^n \subseteq (\mathbf{R}^c)^e, \qquad (sa, ta) \in \mathbf{S}^n \subseteq (\mathbf{R}^c)^e,$$

e portanto $(\mathbf{R}^c)^e$ é uma congruência em S que contém $\mathbf{R}$. Para mostrar que $(\mathbf{R}^c)^e$ é a mais pequena congruência em S que contém $\mathbf{R}$, consideremos a congruência k (em S que contém $\mathbf{R}$). Então $k^c = k$ pelo lema 1.33, e portanto

$$\mathbf{R}^c \subseteq k^c = k.$$

Temos assim que k é uma equivalência em S que contém $\mathbf{R}$, da proposição 1.29, sai que $(R^c)^e \subseteq k$. □

Dadas duas relações de equivalência, ρ, σ, designa-se por $\rho \vee \sigma$ a intersecção de todas as relações de equivalência que contêm ρ e σ (menor relação de equivalência que contém $\rho \cup \sigma$). Vamos ver que $\rho \vee \sigma = (\rho \circ \sigma)^\infty$.

Proposição 1.37. *Sejam ρ, σ duas relações de equivalência num conjunto S [congruências num semigrupo S]. Então, $(a,b) \in \rho \vee \sigma$, se e só se, para algum $n \in \mathbb{N}$, existem $x_1, x_2, ..., x_{2n-1} \in S$, tais que $(a, x_1) \in \rho$, $(x_1, x_2) \in \sigma$, $(x_2, x_3) \in \rho$,...,$(x_{2n-1}, b) \in \sigma$.*

DEMONSTRAÇÃO. O significado deste resultado é $\rho \vee \sigma = (\rho \circ \sigma)^\infty$. Ora das Proposições 1.29 e 1.36, temos $\rho \vee \sigma = R^\infty$, com

$$\begin{aligned} R &= (\rho \cup \sigma) \cup (\rho \cup \sigma)^{-1} \cup 1_S \\ &= \rho \cup \sigma \cup \rho^{-1} \cup \sigma^{-1} \cup 1_S \\ &= \rho \cup \sigma, \end{aligned}$$

pois ρ, σ são relações de equivalência. Por outro lado, como $\rho \subseteq \rho \cup \sigma$ e $\sigma \subseteq \rho \cup \sigma$, vem $\rho \circ \sigma \subseteq (\rho \cup \sigma)^2$. Logo, $(\rho \circ \sigma)^n \subseteq (\rho \cup \sigma)^{2n}$, para $n \geq 1$, então,

$$(\rho \circ \sigma)^\infty \subseteq (\rho \cup \sigma)^\infty = \rho \vee \sigma.$$

Agora, reciprocamente, como ρ, σ são relações de equivalência, $\rho \subseteq \rho \circ \sigma$ e $\sigma \subseteq \rho \circ \sigma$, logo, $\rho \cup \sigma \subseteq \rho \circ \sigma$, assim,

$$\rho \vee \sigma = (\rho \cup \sigma)^{\infty} \subseteq (\rho \circ \sigma)^{\infty}.$$

□

Observação 1.38. Se ρ e σ comutam, então

$$\rho \vee \sigma = (\rho \circ \sigma)^{\infty} = \rho \circ \sigma.$$

6 Ideais e congruências de Rees

Primeiro, se I é um ideal próprio de um semigrupo S, então,

$$\rho_I = (I \times I) \cup 1_S$$

é uma congruência em S. Basta ver que $x\rho_I y$ se e só se $x = y$ ou x e y pertencem a I. É fácil verificar ρ_I é reflexiva, simétrica, transitiva e compatível. O semigrupo quociente é

$$S/\rho_I = \{I\} \cup \{\{x\} : x \in S \backslash I\},$$

em que é conveniente considerar como o semigrupo cujos elementos são I e os elementos de $S\backslash I$. Em S/ρ_I o produto de dois elementos em $S\backslash I$ é o mesmo que o seu produto em S, se este pertencer a $S\backslash I$; caso contrário este produto é I. Uma vez que o elemento I de S/ρ_I é o zero do semigrupo, uma outra forma de pensar em S/ρ_I é como $(S\backslash I) \cup \{0\}$, onde todos os produtos não pertencentes a $S\backslash I$ são zero.

Chamaremos a uma congruência deste tipo, *congruência de Rees*, e se um morfismo $\phi : S \to T$ é tal que $ker\phi$ é uma congruência de Rees dizemos que ϕ é um *morfismo de Rees*. Escrevemos S/I em vez de S/ρ_I, e quando falamos de *Kernel* de um morfismo de Rees significa ideal I em vez da congruência ρ_I.

É importante notar que nem todos os morfismos de semigrupos são deste tipo. Grupos são semigrupos, mas um morfismo $\phi : G \to H$, entre dois grupos não triviais, não pode ser um morfismo de Rees, uma vez que G não tem ideais próprios e H não tem o elemento zero.

7 Equivalências de Green

Se a é um elemento de um semigrupo S, o ideal esquerdo de S mais pequeno que contém a é $Sa \cup \{a\}$, que em 1.2 está convenientemente definido por S^1a; a este ideal chamamos *ideal principal esquerdo gerado por a*. A equivalência $\mathcal{L}$, em S, é definida pela lei $a \mathcal{L} b$ se e só se a e b geram o mesmo ideal principal esquerdo, isto é, se e só se $S^1a = S^1b$. De forma análoga se define equivalência $\mathcal{R}$, pela lei $a \mathcal{R} b$ se e só se $aS^1 = bS^1$. É de verificação rotineira a seguinte caracterização dos elementos das $\mathcal{L}$, $\mathcal{R}$ equivalências:

Proposição 1.39. *Sejam a, b elementos de um semigrupo S. Então $a \mathcal{L} b$ se e só se existem x, y em S^1 tal que $xa = b$, $yb = a$. E ainda, $a \mathcal{R} b$ se e só se existem u, v em S^1 tal que $au = b$, $bv = a$.*

Uma outra propriedade imediata de $\mathcal{L}$ e de $\mathcal{R}$ é:

Proposição 1.40. *$\mathcal{L}$ é uma congruência direita e $\mathcal{R}$ é uma congruência esquerda.*

Demonstração. Seja $a \in S$, $(r, t) \in \mathcal{L}$ e $(f, h) \in \mathcal{R}$, arbitrários. Então, $rS^1 = tS^1$, logo $arS^1 = atS^1$ e assim, $(ar, at) \in \mathcal{L}$. E $S^1f = S^1h$, logo $S^1fa = S^1ha$ e assim, $(fa, ha) \in \mathcal{R}$. □

Designa-se por $\mathcal{H}$ a intersecção das relações $\mathcal{R}$ e $\mathcal{L}$. Como se sabe $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$ é ainda uma relação de equivalência. Por $\mathcal{D}$ designa-se a equivalência $\mathcal{L} \vee \mathcal{R}$. Vamos ver que, para a composição, $\mathcal{L}$ e $\mathcal{R}$ comutam, o que nos permite afirmar, pela Proposição 1.37 que $\mathcal{D} = \mathcal{R} \circ \mathcal{L}$.

Proposição 1.41. *As relações $\mathcal{L}$ e $\mathcal{R}$ comutam.*

Demonstração. Seja S um semigrupo, sejam $a, b \in S$ e suponha-se que $(a, b) \in \mathcal{L} \circ \mathcal{R}$. Então existe $c \in S$, tal que $a \mathcal{L} c$ e $c \mathcal{R} b$. Logo existem $x, y, u, v \in S^1$, tais que

$$xa = c, \quad cu = b,$$

$$yc = a, \quad bv = c.$$

Seja $d = ycu \in S$, então

$$au = ycu = d, \quad dv = ycuv = ybv = yc = a;$$

logo $a \mathcal{R} d$. Por outro lado,

$$yb = ycu = d, \quad xd = xycu = xau = cu = b,$$

logo $d \mathcal{L} b$. Assim, $(a, b) \in \mathcal{R} \circ \mathcal{L}$. A inclusão recíproca segue um caminho análogo. Assim, $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$. □

Definimos agora uma relação de equivalência, simultaneamente esquerda e direita, em S, da seguinte forma : $a \mathcal{I} b$ se e só se $S^1 a S^1 = S^1 b S^1$. Como facilmente se verifica $\mathcal{L} \subseteq \mathcal{I}$ e $\mathcal{R} \subseteq \mathcal{I}$. Como $\mathcal{D}$ é a menor relação de equivalência que contém $\mathcal{L}$ e $\mathcal{R}$, então $\mathcal{D} \subseteq \mathcal{I}$. O seguinte resultado vai permitir-nos concluir que $\mathcal{D} = \mathcal{I}$ em todo o semigrupo finito.

Proposição 1.42. *Se S é um semigrupo periódico, então $\mathcal{D} = \mathcal{I}$.*

Demonstração. Sejam $a, b \in S$, tais que $a \mathcal{I} b$. Então existem $x, y, u, v \in S^1$, tais que

$$xay = b, \quad ubv = a. \tag{1.16}$$

Precisamos, agora, de encontrar um elemento $c \in S$, tal que $a \mathcal{L} c$, $c \mathcal{R} b$. Resulta da equação (1.16), que

$$\begin{aligned} a &= (ux)a(yv) = (ux)^2 a(yv)^2 = (ux)^3 a(yv)^3 = ... \\ b &= (xu)b(vy) = (xu)^2 b(vy)^2 = (xu)^3 b(vy)^3 = ... \end{aligned}$$

Como S é periódico, pela Proposição 1.20, podemos encontrar m, tal que $(ux)^m$ é idempotente. Assim, seja $c = xa$, então

$$a = (ux)^m a(yv)^m = (ux)^m (ux)^m a(yv)^m = (ux)^m a = (ux)^{m-1} uc,$$

logo $a \mathcal{L} c$. Por outro lado, $cy = xay = b$ e se escolhermos n, tal que $(vy)^n$ é idempotente, tem-se

$$\begin{aligned} c &= xa = x(ux)^{n+1} a(yv)^{n+1} = (xu)^{n+1} xay(vy)^n v \\ &= (xu)^{n+1} b(vy)^{2n} v = (xu)^{n+1} b(vy)^{n+1} (vy)^{n-1} v \\ &= b(vy)^{n-1} v. \end{aligned}$$

Logo $c \mathcal{R} b$, como pretendíamos. □

À custa da relação de ordem parcial dada pela inclusão de conjuntos vamos definir uma pré-ordem, $\leq_R$, nas classes de $\mathcal{R}$, da forma $s \leq_R t$ se e só se $R_s \leq_R R_t$ se e só se $sS^1 \subseteq tS^1$. De forma análoga se definem pré-ordens em $\mathcal{L}$ e em $\mathcal{I}$.

Estrutura das $\mathcal{D} - classes$: Cada $\mathcal{D} - classe$, num semigrupo S, é a reunião disjunta de $\mathcal{L} - classes$ e, também, a reunião disjunta de $\mathcal{R} - classes$. Seja D uma $\mathcal{D} - classe$ e $a \in D$, então $a \in R$, para alguma $\mathcal{R} - classe$. Seja $b \in S$, tal que

$b \in R$, então $b\mathcal{R}a$ e $a\mathcal{L}a$, logo $b\mathcal{D}a$, isto é $b \in D$. O mesmo raciocínio se pode aplicar às $\mathcal{L} - classes$.

A intersecção de uma $\mathcal{L} - classe$ com uma $\mathcal{R} - classe$ é, ou vazia, ou uma $\mathcal{H} - classe$. Como $\mathcal{D} = \mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$, tem-se

$$a\mathcal{D}b \Leftrightarrow R_a \cap L_b \neq \emptyset \Leftrightarrow L_a \cap R_b \neq \emptyset.$$

Pode visualizar-se uma $\mathcal{D} - classe$ como uma "caixa-de-ovos"em que cada linha representa uma $\mathcal{R}-classe$ e cada coluna representa uma $\mathcal{L}-classe$ e cada "célula"representa uma $\mathcal{H} - classe$.

		$L_a = L_c$		L_b	
$R_a = R_b$		H_a		H_b	
R_c		H_c			

Se D é uma $\mathcal{D} - classe$ arbitrária num semigrupo S e se $a, b \in D$ são tais que $a \mathcal{L} b$, então por definição de $\mathcal{L}$ existem $t, t' \in S^1$, tais que

$$ta = b, \quad t'b = a.$$

A translação esquerda $\lambda_t : S \to S$, $x \to tx$, aplica R_a em R_b pois, se $x \in R_a$, então, pela Proposição 1.40, $tx \mathcal{R} ta$, logo, $tx \in R_{ta} = R_b$. De forma semelhante se prova que $\lambda_{t'}$ aplica R_b em R_a. A composição $\lambda_t\lambda_{t'} : R_a \to R_a$ é a aplicação identidade em R_a e $\lambda_{t'}\lambda_t : R_b \to R_b$ é a identidade em R_b. Então, $\lambda_{t|_{R_a}}$ e $\lambda_{t'|_{R_b}}$ são bijecções mutuamente inversas de R_a em R_b e de R_b em R_a, respectivamente. Ainda se pode deduzir que se $x \in R_a$ então o elemento $y = x\lambda_t$ de R_b tem a propriedade $y = tx$, $x = t'y$. Então $x \mathcal{L} y$, logo a aplicação λ_t preserva a $\mathcal{L}-classe$, aplica bijectivamente cada $\mathcal{H}-classe$ de R_a, numa $\mathcal{H}-classe$ de R_b, mantendo-se na $\mathcal{L}-classe$. O mesmo se conclui de $\lambda_{t'}$. Raciocínio semelhante nos levaria a concluir o mesmo acerca das translações $\rho_s : S \to S$, $x \to xs$ e $\rho'_s : S \to S$, $x \to xs'$, translações que preservam as $\mathcal{R} - classes$ e aplicam bijectivamente uma $\mathcal{H} - classe$ noutra $\mathcal{H} - classe$ e uma $\mathcal{L} - classe$ noutra $\mathcal{L} - classe$. Podemos então enunciar a seguinte

Proposição 1.43. *Sejam a, b elementos $\mathcal{R} - equivalentes$ (respectivamente $\mathcal{L} - equivalentes$), num semigrupo S e sejam $s, s' \in S^1$ (respectivamente $t, t' \in S^1$), tais que, $as = b$, $bs' = a$ (respectivamente $ta = b$, $t'b = a$). Então, as translações direitas*

(respectvamente, esquerdas) $\rho_{s|_{L_a}}$, $\rho_{s'|_{L_b}}$ *(respectivamente,* $\lambda_{t|_{R_a}}$, $\lambda_{t'|_{R_b}}$*) são bijecções mutuamente inversas, que preservam a* $\mathcal{R}-$*classe (respectivamente,* $\mathcal{L}-$*classe) de* L_a *(respectivamente* R_a*) para* L_b*(respectivamente* R_b*) e de* L_b*(respectivamente* R_b*) para* L_a *(respectivamente* R_a*).*

Daqui resulta,

Lema 1.44. *Se* a, b *são elementos* $\mathcal{D}-$*equivalentes num semigrupo* S*, então* $|H_a| = |H_b|$.

Demonstração. Seja $c \in S$, tal que $a \,\mathcal{R}\, c$ e $c \,\mathcal{L}\, b$, com $as = c$, $cs' = a$, $tc = b$, $t'b = c$. Pelas considerações anteriores $\rho_s\lambda_t : x \to txs$ é bijecção entre H_a e H_b (cuja inversa é $\lambda'_t\rho'_s : y \to t'ys'$). Logo, $|H_a| = |H_b|$. □

Do que foi exposto anteriormente, sabemos que para $a \in S$, $\rho_s : x \to xs$, aplica bijectivamente H_a em H_{as}. Ora, se tivermos, em particular, $a \,\mathcal{H}\, as$, então ρ_s aplica bijectivamente H_a em si própria. O mesmo se verifica para $\lambda_t : x \to tx$, que aplica H_a em H_{ta}. Se $a \,\mathcal{H}\, ta$, então λ_t aplica H_a em si própria, bijectivamente. Então podemos afirmar,

Lema 1.45. *Sejam* $x, y \in S$ *(semigrupo). Se* $xy \in H_x$*, então* $\rho_{y|_{H_x}}$ *é uma bijecção de* H_x *em si própria. Se* $xy \in H_y$ *então* $\lambda_{x|_{H_y}}$ *é uma bijecção de* H_y *em si própria.*

Daqui resulta o seguinte Teorema (de Green)

Teorema 1.46. *Se* H *é uma* $\mathcal{H}-$*classe num semigrupo* S*, então, ou* $H^2 \cap H = \emptyset$*, ou* $H^2 = H$*, e* H *é subgrupo de* S.

Demonstração. Suponhamos que $H^2 \cap H \neq \emptyset$, então existem $a, b \in H$, tais que $ab \in H$. Pelo Lema 1.44, ρ_b e λ_a são bijecções de H em si própria. Assim, $hb \in H$ e $ah \in H$, qualquer que seja $h \in H$. Então, pelo Lema 1.44, λ_h e ρ_h são bijecções de H em si própria. Logo, $Hh = hH = H$, para todo o $h \in H$, ou seja $H^2 = H$ e H é grupo, subgrupo de S. □

O resultado seguinte é consequência deste teorema.

Corolário 1.47. *Se* $e \in S$ *é idempotente, então* H_e *é subgrupo de* S*. Nenhuma* $\mathcal{H}-$*classe em* S *pode conter mais do que um idempotente.*

Demonstração. Como $H_e^2 \cap H_e \neq \emptyset$ (pois $ee = e$) então, H_e é subgrupo de S. Logo, só tem um idempotente, o elemento neutro. □

Definição 1.48. Um elemento a, num semigrupo S, diz-se *regular* se existir $x \in S$, tal que $axa = a$.

Vamos ver que numa $\mathcal{D} - classe$, se existir um elemento regular, então todos os seus elementos são regulares.

Proposição 1.49. *Se $a \in S$ é regular, então todos os elementos de D_a são regulares.*

Demonstração. Temos $axa = a$, para algum $x \in S$. Se $c \in R_a$, então existem $y, z \in S^1$, tais que $ay = c$ e $cz = a$. Logo, $c = ay = axay = axc = c(zx)c$, logo, c é regular. De modo análogo se prova que qualquer elemento de uma $\mathcal{L} - classe$ de um elemento regular é regular. □

Uma $\mathcal{D} - classe$ diz-se *regular* se os seus elementos são todos regulares. Caso contrário diz-se irregular.

Proposição 1.50. *Numa $\mathcal{D} - classe$ regular todas as $\mathcal{L} - classes$ e todas as $\mathcal{R} - classes$ contêm idempotentes.*

Demonstração. Se a pertence a uma $\mathcal{D} - classe$ regular, então existe $x \in S$, tal que $axa = a$. Então, $axax = ax$ e $ax \; \mathcal{R} \; a$, ou seja ax é um idempotente em R_a. De forma semelhante se prova que xa é um idempotente em L_a. □

Proposição 1.51. *Um idempotente e, num semigrupo S é uma identidade esquerda em R_e e uma identidade direita em L_e.*

Demonstração. Se $b \in L_e$, então $b = xe$, para algum $x \in S^1$. Então,

$$be = (xe)e = xe^2 = xe = b.$$

De modo análogo se prova que $ea = a$, para todo o $a \in R_e$. □

Corolário 1.52. *Se uma $\mathcal{D} - classe$ D contém um idempotente, então todas as $\mathcal{R} - classes$ e $\mathcal{L} - classes$ em D contêm um idempotente.*

Demonstração. Seja e um idempotente na classe D_e, então e é regular, pois $eee = e$. Pela Proposição 1.50, tem-se o pretendido. □

Definição 1.53. Dado um semigrupo S e $a \in S$, diz-se que $a' \in S$ é um inverso de a, se $aa'a = a$ e $a'aa' = a'$.

Daqui resulta que, se um elemento tem um inverso, então é regular. Por outro lado, se existir $x \in S$, tal que $axa = a$, então $a' = xax$ é um inverso de a,

$$aa'a = axaxa = axa = a,$$
$$a'aa' = xaxaxax = xax = a',$$

isto é, se um elemento é regular tem um inverso. Denotemos por $V(a)$ o conjunto dos inversos de um elemento a.

Teorema 1.54. *Seja a um elemento de D, uma $\mathcal{D}-$classe regular , num semigrupo S.*

(1) *Se $a' \in V(a)$, então $a' \in D$ e as duas $\mathcal{H}-$classes $R_a \cap L_{a'}$, $L_a \cap R_{a'}$ contêm, respectivamente, os idempotentes aa' e $a'a$,*

		L_a		$L_{a'}$	
R_a		a		aa'	
$R_{a'}$		$a'a$		a'	

(2) *Se $b \in D$ é tal que $R_a \cap L_b$ e $L_a \cap R_b$ contêm os idempotentes e, f, respectivamente, então H_b contém um inverso a^*, de a, tal que $aa^* = e$, $a^*a = f$,*

		L_a		L_b	
R_a		a		e	
R_b		f		b , a^*	

(3) *Nenhuma $\mathcal{H}-$classe contém mais que um inverso de a.*

Demonstração. (1) Se $aa'a = a$ e $a'aa' = a'$, então $a \mathcal{R}\, aa'$, $a' \mathcal{R}\, a'a$, $a \mathcal{L}\, a'a$, $a' \mathcal{L}\, aa'$. Assim, $aa' \in R_a \cap L_{a'}$ e $a'a \in L_a \cap R_{a'}$.

(2) Como $e \in R_a \cap L_b$, então, $e \in R_a$ e $ea = a$, pois e é uma identidade esquerda em $R_e = R_a$. Por outro lado, como $f \in L_a \cap R_b$, então $f \in L_a$, logo,

$L_a = L_f$. Assim, $af = a$, pois f é identidade direita em L_f. De $a \mathcal{R} e$, resulta que existe $x \in S^1$, tal que $ax = e$. Fazemos $a^* = fxe$.

$$aa^*a = afxea = axa = ea = a,$$
$$a^*aa^* = fxeafxe = fxafxe = fxaxe = fxe^2 = fxe = a^*.$$

Assim, a^* é um inverso de a. Ainda se tem,

$$aa^* = afxe = axe = e^2 = e$$

Como $f = ya$, para algum $y \in S^1$, pois $f \in L_a$,

$$a^*a = fxea = fxa = yaxa = yea = ya = f.$$

Finalmente, como também se tem $(fx)e = a^*$ e $f(xe) = a^*$, então $L_{a^*} = L_e$, $R_f = R_{a^*}$. Logo,

$$a^* \in L_e \cap R_f = L_b \cap R_b = H_b.$$

(3) Suponhamos que a' e a^* são inversos de a em H_b. Então $aa'aa' = aa'$, $aa^*aa^* = aa^*$, $a'aa'a = a'a$, $a^*aa^*a = a^*a$, isto é, aa', aa^* são idempotentes em $R_a \cap L_b$, logo, são iguais e, $a'a$, a^*a são idempotentes em $L_a \cap R_b$, assim, são também iguais. Finalmente, $a^* = a^*aa^* = a^*aa' = a'aa' = a'$. □

Proposição 1.55. *Sejam e, f idempotentes num semigrupo S. Então, $(e, f) \in \mathcal{D}$ se e só se existe um elemento $a \in S$ e um seu inverso a', tais que $a'a = e$, $a'a = f$*

		L_f		L_e	
R_e		a		e	
R_f		f		a'	

Demonstração. Se $e, f \in \mathcal{D}$, então a sua $\mathcal{D} - classe$ é regular. Seja $a \in R_e \cap L_f$, pelo Teorema 1.54, existe um inverso a' de a em $R_f \cap L_e$, tal que $aa' = e$, $a'a = f$. Se existem $a, a' \in S$ inversos, tais que $aa' = e$, $a'a = f$, então, pelo Teorema 1.54 (1), $e = aa' \in R_a$ e $f = a'a \in L_a$. Assim, $e \mathcal{R} a$, $a \mathcal{L} f$, logo, $e \mathcal{D} f$. □

Vamos agora ver que duas $\mathcal{H} - classes$, subgrupos de S, na mesma $\mathcal{D} - classe$ são isomorfas.

Proposição 1.56. *Sejam H e K duas $\mathcal{H}-$classes grupos, na mesma $\mathcal{D}-$classe, então H e K são isomorfas.*

DEMONSTRAÇÃO. Seja e o elemento neutro de H, f o elemento neutro de K, que são idempotentes. Seja $a \in R_e \cap L_f$ e $a' \in R_f \cap L_e$ o único inverso de a nesta $\mathcal{H}-$*classe*. Então, $aa' = e$, $a'a = f$, $ea = af = a$, $a'e = fa' = a'$. É fácil verificar que $\phi : H \to K$, $x \to a'xa$ é um isomorfismo de H em K. □

Lema 1.57. *Sejam a, b elementos de D, uma $\mathcal{D}-$classe. Então, $ab \in R_a \cap L_b$ se e só se $L_a \cap R_b$ contém um idempotente.*

DEMONSTRAÇÃO. Suponha-se que $ab \in R_a \cap L_b$. Então existe $c \in S^1$, tal que, $abc = a$ e, pela Proposição 1.43, $\rho_c : x \to xc$ aplica bijectivamente H_b em $L_a \cap R_b$. Assim, $bc \in L_a \cap R_b$. Por outro lado, $\rho_b : y \to yb$ aplica bijectivamente $L_a \cap R_b$ em H_b e são inversas. Logo, bc é idempotente, pois

$$(bc)^2 = b\rho_c\rho_b\rho_c = b\rho_c = bc.$$

Reciprocamente, se $L_a \cap R_b$ contém um idempotente e, então $eb = b$ e a translação $x \to xb$ aplica bijectivamente H_a em $R_a \cap L_b$. Em particular, $ab \in R_a \cap L_b$. □

8 Semigrupos regulares

Num semigrupo regular S temos uma forma útil de olhar para as equivalências $\mathcal{L}$ e $\mathcal{R}$. Primeiro, se S é *regular* então $a = axa \in aS$, e analogamente $a \in Sa$, $a \in SaS$. Por esta razão podemos afirmar que

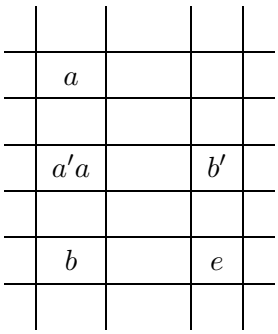
$$\begin{aligned} a\mathcal{L}b &\quad \text{se e só se} \quad Sa = Sb, \\ a\mathcal{R}b &\quad \text{se e só se} \quad aS = bS, \\ a\mathcal{J}b &\quad \text{se e só se} \quad SaS = SbS. \end{aligned}$$

Proposição 1.58. *Sejam a, b elementos de um semigrupo regular S. Então*

(1) $(a, b) \in \mathcal{L}$ *se e só se existem a' pertencente a $V(a)$ e b' pertencente a $V(b)$ tal que $aa' = b'b$;*

(2) $(a, b) \in \mathcal{R}$ *se e só se existem a' pertencente a $V(a)$ e b' pertencente a $V(b)$ tal que $aa' = bb'$;*

(3) $(a,b) \in \mathcal{H}$ *se e só se existem* a' *pertencente a* $V(a)$ *e* b' *pertencente a* $V(b)$ *tal que* $aa' = b'b$ *e* $aa' = bb'$.



DEMONSTRAÇÃO. Parte (1): Suponhamos que $(a,b) \in \mathcal{L}$. Se $a' \in V(a)$ então $a'a$ é idempotente em $L_a = L_b$. A $\mathcal{R} - classe$ contém, pela Proposição 1.50, pelo menos um elemento idempotente e, e então, pelo Teorema 1.54 (2), a $\mathcal{H} - classe$ $R_{a'a} \cap L_e$ contém um inverso b' de b com a propriedade $b'b = a'a$ (e $bb' = e$). Mostrámos a seguinte implicação

$$(a,b) \in \mathcal{L} \Rightarrow (\forall a' \in V(a))(\exists b' \in V(b)) \;\; a'a = b'b. \tag{1.17}$$

Reciprocamente, se $a'a = b'b$ para algum a' pertencente a $V(a)$ e algum b' pertencente a $V(b)$ então, pelo Teorema 1.54 (1), $a\mathcal{L}a'a$ e $b'b\mathcal{L}b$, por transitividade temos $a\mathcal{L}b$.

Parte (2): De forma análoga à anterior conseguimos provar que

$$(a,b) \in \mathcal{L} \Rightarrow (\forall a' \in V(a))(\exists b' \in V(b)) \;\; aa' = bb'. \tag{1.18}$$

Parte (3): Suponhamos que $a\mathcal{H}b$ e que $a' \in V(a)$. Assim, $aa' \in R_a = R_b$ e $aa' \in L_a = L_b$. Logo, pelo Teorema 1.54 (2), a $\mathcal{H} - classe$ $L_{a'a} \cap R_{a'a}$ contém um inverso b' de b tal que $bb' = aa'$ e $b'b = a'a$. Provámos a implicação

$$(a,b) \in \mathcal{H} \Rightarrow (\forall a' \in V(a))(\exists b' \in V(b)) \quad a'a = b'b \;\text{ e }\; aa' = bb'. \tag{1.19}$$

A implicação contrária é obvia. □

Nesta altura podemos concluir sobre a correspondência entre congruências e morfismos, iniciada na secção congruências, com a seguinte versão do Lema de Lallement.

Lema 1.59. *Seja* $\phi : S \to T$ *um morfismo entre um semigrupo regular* S *e um semigrupo* T. *Então* $im\phi$ *é regular. Se* f *é idempotente em* $im\phi$ *então existe* e, *idempotente em* S, *tal que* $e\phi = f$.

9 Semigrupos inversos

Sejam X e Y dois quaisquer conjuntos. Uma *função parcial* f de X para Y é uma função de um subconjunto de X num subconjunto de Y. Ao subconjunto de X, formado por todos os elementos $x \in X$ para os quais $f(x)$ está definida, chamamos *domínio* de f, e denotamos por dom f. A *imagem* de f é o subconjunto im $f = f(\text{dom} f)$ de Y.

Há duas classes de funções parciais especialmente importantes. Para quaisquer dois conjuntos X e Y existe uma única *função parcial vazia de X para Y* que denotamos por 0_{YX}. Para qualquer subconjunto A de X a função identidade em A, denotada por 1_A, é uma função parcial de X em si próprio. Designamos tais funções parciais por *identidades parciais*. A função identidade parcial de dom$f$ denotamos por $\mathbf{d}(f)$ e a função identidade parcial de im$f$ denotamos por $\mathbf{r}(f)$. A função identidade 1_X em X e a função identidade $1_\emptyset$ num subconjunto vazio de X, que é a função vazia de X nele próprio, são especialmente importantes. Quando é claro o conjunto subjacente X, denotamos estas funções por 1 e 0, respectivamente.

Daremos especial atenção às funções parciais que induzem bijecções entre os seus domínios e imagens; chamamos a essas funções parciais, *bijecções parciais*. Todas as identidades parciais e funções vazias são bijecções parciais. Se f for uma bijecção parcial de X para Y então, denotamos por f^{-1} a bijecção parcial de Y para X que é a *inversa* de f. Assim, o domínio de f^{-1} é imagem de f e a sua imagem é dom$f$.

A colecção de todas as bijecções parciais entre conjuntos formam uma categoria, mas nós estamos especialmente interessados no conjunto das bijecções parciais de um conjunto X nele próprio, em particular de $\mathbb{N}$ em si próprio. Isto forma um monoide, que denotamos por $I(X)$, chamado *monoide simétrico inverso*.

Relembramos que num semigrupo, um idempotente é qualquer elemento igual ao seu quadrado.

Apresentamos de seguida alguns resultados cuja demonstração se pode encontrar, por exemplo, em [26].

Proposição 1.60. *Seja $I(X)$ o monoide simétrico inverso no conjunto X. Então os idempotentes de $I(X)$ são precisamente as identidades parciais em X. Em particular, os idempotentes formam um subsemigrupo comutativo.*

Definição 1.61. Seja S um semigrupo, S pertence à classe dos *semigrupos inversos* se:

(1) S é regular. Isto é, para todo elemento $a \in S$ existe x em S, que chamamos *inverso de a*, tal que $a = axa$ e $x = xax$;

(2) Os idempotentes de S comutam.

Os monóides simétricos inversos são semigrupos inversos.

Teorema 1.62. *Seja S um semigrupo regular. Então os idempotentes de S comutam se e só se, cada elemento de S tem um único inverso.*

Os semigrupos inversos são então os semigrupos S em que, para cada elemento $s \in S$, existe um único elemento $s^{-1} \in S$ tal que $s = ss^{-1}s$ e $s^{-1} = s^{-1}ss^{-1}$. Ao elemento s^{-1} chamamos *inverso* de s em S. Um *subsemigrupo inverso* de um semigrupo inverso é um subsemigrupo fechado sob os inversos, ou seja, que contém os inversos dos seus elementos.

Proposição 1.63. *Seja S um semigrupo inverso.*

(1) *Para qualquer $s \in S$, tanto $s^{-1}s$ como ss^{-1} são idempotentes e $s(s^{-1}s) = s$ e $(ss^{-1})s = s$.*

(2) *$(s^{-1})^{-1} = s$ para qualquer $s \in S$.*

(3) *Para qualquer idempotente e de S e qualquer $s \in S$ o elemento $s^{-1}es$ é um idempotente.*

(4) *Se e for um idempotente em S então $e^{-1} = e$.*

(5) *$(s_1 \dots s_n)^{-1} = s_n^{-1} \dots s_1^{-1}$ para todos $s_1, \dots, s_n \in S$ em que $n \geq 2$.*

Demonstração.

(1) Comecemos por observar que $(s^{-1}s)^2 = s^{-1}(ss^{-1}s) = s^{-1}s$. Uma demonstração análoga mostra que ss^{-1} é um idempotente.

(2) É claro que s é solução das equações $s^{-1} = s^{-1}xs^{-1}$ e $x = xs^{-1}x$. Da unicidade dos inversos sai o resultado.

(3) Temos que $(s^{-1}es)^2 = s^{-1}e(ss^{-1})es = s^{-1}e^2(ss^{-1}s) = s^{-1}es$, usando o facto de que os idempotentes comutam.

(4) Imediato.

(5) O caso $n = 2$ é imediato da definição e do facto de os idempotentes comutarem. O caso geral demonstra-se por indução.

□

Os idempotentes ss^{-1} e $s^{-1}s$ comportam-se como identidade esquerda e direita, respectivamente, para o elemento s, pela Proposição 1.63. Podemos escrever $\mathbf{d}(s) = s^{-1}s$ e $\mathbf{r}(s) = s^{-1}s$. O conjunto de todos os idempotentes de S é denotado por $E(S)$ e, se A for um subconjunto de S, então $E(A) = A \cap E(S)$.

Lema 1.64. *Seja S um semigrupo inverso.*

(1) *Para todo idempotente e e elemento s existe um idempotente f de tal modo que $es = sf$.*

(2) *Para todo idempotente e e elemento s existe um idempotente f de tal modo que $se = fs$.*

Demonstração. Provaremos (1); a demonstração de (2) é similar. Seja $f = s^{-1}es$, um idempotente, pela Proposição 1.63. Então,

$$sf = s(s^{-1}es) = (ss^{-1})es = e(ss^{-1})s = es.$$

□

Seja S um semigrupo inverso. Se S tem uma identidade, então podemos dizer que S é um *monoide inverso*; se tiver um elemento zero então podemos dizer que S é um *semigrupo inverso com zero*. Todo semigrupo (inverso) pode ser convertido num monoide (inverso) ou num semigrupo (inverso) com zero, juntando-lhe uma identidade ou um zero num procedimento análogo ao que vimos nas Definições 1.6 e 1.7.

Definimos a relação $\leq$ num semigrupo inverso S de seguinte modo:

$$s \leq t \Leftrightarrow s = te$$

para algum idempotente e. Esta relação de ordem é chamada *ordem parcial natural* em S. Apresentamos a seguir duas proposições importantes que envolvem esta relação.

Lema 1.65. *Seja S um semigrupo inverso. Então, são equivalentes as seguintes condições:*

(1) $s \leq t$.

(2) $s = ft$, *para algum idempotente* f.

(3) $s^{-1} \leq t^{-1}$.

(4) $s = ss^{-1}t$.

(5) $s = ts^{-1}s$.

DEMONSTRAÇÃO.

(1) $\Rightarrow$ (2). Seja $s = te$. Então $s = ft$ para algum idempotente f, pelo Lema 1.64.

(2) $\Rightarrow$ (3). Seja $s = ft$ para algum f idempotente. Então $s^{-1} = t^{-1}f$. Logo, pela definição, $s^{-1} \leq t^{-1}$.

(3) $\Rightarrow$ (4). Seja $s^{-1} \leq t^{-1}$. Então, $s^{-1} = t^{-1}e$, para algum idempotente e. Considerando os inversos, obtemos $s = et$. Mas $es = s$, e portanto, $ess^{-1} = ss^{-1}$. Logo, $s = ss^{-1}t$.

(4) $\Rightarrow$ (5). Seja $s = ss^{-1}t$. Então, pelo Lema 1.64, $s = te$ para algum idempotente e. Mas, $se = s$ e $s^{-1}se = s^{-1}s$. Logo, $s = ts^{-1}s$.

(5) $\Rightarrow$ (1). Imediato.

□

Proposição 1.66. *Seja S um semigrupo inverso.*

(1) *A relação $\leq$ é uma ordem parcial em S.*

(2) *Para quaisquer idempotentes $e, f \in S$ temos $e \leq f$, se e só se, $e = ef = fe$.*

(3) *Se $s \leq t$ e $u \leq v$, então $su \leq tv$.*

(4) *Se $s \leq t$ então $s^{-1}s \leq t^{-1}t$ e $ss^{-1} \leq tt^{-1}$.*

(5) *$E(S)$ é um ideal ordenado de S.*

DEMONSTRAÇÃO.

(1) Como $s = s(s^{-1}s)$, a relação é reflexiva. Fazendo $s \leq t$ e $t \leq s$. Então, $s = ts^{-1}s$ e $t = st^{-1}t$, e portanto,

$$s = ts^{-1}s = st^{-1}ts^{-1}s = st^{-1}t = t.$$

Logo, a relação é anti-simétrica. Suponhamos agora que $s \leq t$ e $t \leq u$. Então, $s = te$ e $t = uf$, para alguns idempotentes e e f. Assim, $s = te = (uf)e = u(fe)$. Logo, $s \leq u$.

(2) Suponhamos que $e \leq f$. Então, $e = fi$, para algum idempotente i. Mas então, $fe = e$ e portanto, $e = fe = ef$. O recíproco é óbvio.

(3) Seja $s \leq t$ e $u \leq v$. Então, existem idempotentes e e f tais que $s = te$ e $u = vf$. Logo, $su = tevf$. Pelo Lema 1.64, $ev = vi$ para algum idempotente i. Logo, $su = tv(if)$ e portanto, $su \leq tv$.

(4) É imediato do Lema 1.65(3) e do (3) anterior.

(5) Imediato da definição de ordem parcial natural e do facto de que $E(S)$ é fechado para a multiplicação.

□

Seja S um semigrupo e $\leq$ uma ordem parcial definida em S. Então, $\leq$ diz-se *compatível* relativamente à multiplicação, se para todos $a, b, c, d \in S$ temos $a \leq b$ e $c \leq d$ implica que $ac = bd$. Neste caso, o semigrupo S diz-se *parcialmente ordenado* por $\leq$.

Observe-se que se T for um subsemigrupo inverso de S, então a ordem parcial natural definida em T coincide com a restrição a T da ordem parcial natural em S.

Definição 1.67. Um semigrupo inverso diz-se *completamente semisimples* se a ordem natural parcial é uma igualdade quando restringida a qualquer $\mathcal{D} - classe$.

Teorema 1.68. *Seja S um semigrupo inverso. Se D é uma $\mathcal{D} - classe$ de S, então a restrição da ordem parcial natural a D ou é uma igualdade ou para cada $b \in D$ existe $a \in D$ tal que $a < b$. Em particular, o semigrupo inverso S ou é semisimples completo ou existem dois elementos $a, b \in S$ distintos, $\mathcal{D} - relacionados$, tais que $a < b$.*

Consideremos as seguintes propriedades adicionais dos semigrupos inversos, cujas demonstrações podem ser encontradas em [26].

Proposição 1.69. *Seja ρ uma congruência num semigrupo inverso S.*

(1) *Se $(s, t) \in \rho$ então*

$$(s^{-1}, t^{-1}) \in \rho, \quad (s^{-1}s, t^{-1}t) \in \rho \quad \text{e} \quad (ss^{-1}, tt^{-1}) \in \rho.$$

(2) *Se $(s, e) \in \rho$, em que e é idempotente, então*

$$(s, s^{-1}) \in \rho, \quad (s, s^{-1}s) \in \rho \quad \text{e} \quad (s, ss^{-1}) \in \rho.$$

Definindo num semigrupo S, $\theta : X^\dagger \to S$ (considerando $X = S$ como um conjunto e denotando por $X^\dagger$ o semigrupo livre em X) por $\theta(s_1, \ldots, s_n) = s_1 \ldots s_n$, considerando ρ uma relação em $X^\dagger$, então, o semigrupo $X^\dagger/ker\theta$ denota-se por $\langle X/\rho \rangle$, temos

Proposição 1.70. *Seja S um semigrupo gerado por $\{s_i : i \in I\}$, e seja X o conjunto $\{x_i : i \in I\}$. Seja $\theta : X^\dagger \to S$ o homomorfismo que aplica x_i em s_i. Seja ρ uma relação em $X^\dagger$ tal que $\theta(u) = \theta(v)$ para todo $(u, v) \in \rho$. Então, S é uma imagem homomorfa de $\langle X : \rho \rangle$.*

Vamos agora introduzir um novo conceito, o de *unitário*. Um subconjunto A de um semigrupo inverso S diz-se *unitário esquerdo* (resp. *direito*) se $a \in A$, $s \in S$ e $as \in A$ (resp. $sa \in A$) implicar $s \in A$. Um subconjunto diz-se *unitário* se for simultaneamente unitário direito e esquerdo. Dizemos que um semigrupo inverso é *E-unitário*, sempre que e é um idempotente e $e \leq s$, então s é um idempotente.

Proposição 1.71. *Seja S um semigrupo inverso. Então, as seguintes condições são equivalentes:*

(1) *$E(S)$ é unitário esquerdo.*

(2) *$E(S)$ é unitário direito.*

(3) *Se e for idempotente e $e \leq s$ então s é idempotente.*

Demonstração.

(1) $\Rightarrow$ (2). Suponhamos que $E(S)$ é unitário esquerdo e $se \in E(S)$ com $s \in E(S)$. Então, $se = fs$ para algum idempotente f, pelo Lema 1.64. Assim, s é um idempotente, uma vez que S é unitário esquerdo. Logo, S é unitário direito.

(2) $\Rightarrow$ (3). Suponhamos que $E(S)$ é unitário direito e $e \leq s$ para algum e idempotente. Então, $e = se$ e portanto, s é um idempotente.

(3) $\Rightarrow$ (1). Seja $es = f$ um idempotente. Então, $f \leq s$ e portanto, s é um idempotente.

□

Consideremos agora as aplicações $\mathbf{d}, \mathbf{r} : S \to E(S)$, em que $E(S)$ é o conjunto de todos os idempotentes do semigrupo S, definidas do seguinte modo:

$$\mathbf{d}(s) = s^{-1}s \qquad \text{e} \qquad \mathbf{r}(s) = ss^{-1}$$

Sejam s, t dois quaisquer elementos de um semigrupo inverso S. Então o *produto restrito* $s \cdot t$ existe apenas quando $s^{-1}s = tt^{-1}$, e nesse caso é igual a st. Assim, $s \cdot t$ existe quando $\mathbf{d}(s) = \mathbf{r}(t)$

Lema 1.72. *Seja S um semigrupo inverso. Se existir $s \cdot t$ então $\boldsymbol{d}(s \cdot t) = \boldsymbol{d}(t)$ e $\boldsymbol{r}(s \cdot t) = \boldsymbol{r}(s)$, qualquer que seja s, t pertencentes a S.*

Demonstração. Da definição,

$$\mathbf{d}(s \cdot t) = t^{-1}s^{-1}st$$

e $t^{-1}s^{-1}st = t^{-1}t$ uma vez que $s^{-1}s = tt^{-1}$. □

A demonstração do outro caso é similar.

Retomando a equivalência $\mathcal{H}$ introduzida anteriormente como sendo $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$. Dizemos que um semigrupo inverso é *combinatorial* se $\mathcal{H}$ for a relação de igualdade.

A $\mathcal{H}$-relação é associada à presença de subgrupos num semigrupo, o que significa um subsemigrupo que é também um grupo. Para cada idempotente e de S, o subconjunto eSe é um subsemigrupo com identidade e, chamado *submonóide local*.

Retomando também a equivalência $\mathcal{D}$ introduzida anteriormente como sendo $\mathcal{D} = \mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$, surge-nos o seguinte resultado.

Proposição 1.73. *Seja S um semigrupo inverso.*

(1) *Seja $(e, f) \in E(S)$. Então $e\mathcal{D}f$ se e só se existir $a \in S$ tal que $a^{-1}a = f$ e $aa^{-1}e$;*

(2) *Sejam $(s, t) \in S$. Então $(s, t) \in \mathcal{D}f$ se e só se existirem elementos $a, b \in S$ tal que*

$$\boldsymbol{d}(a) = \boldsymbol{d}(t), \quad \boldsymbol{r}(a) = \boldsymbol{d}(s), \quad \boldsymbol{d}(b) = \boldsymbol{r}(t), \quad \boldsymbol{r}(b) = \boldsymbol{r}(s)$$

com $t = b^{-1} \cdot s \cdot a$.

(3) *Se $s = a_1 \cdot \ldots \cdot a_n$, então $(s, a_i) \in \mathcal{D}$ para todo $i = 1, \ldots, n$.*

Demonstração. (1) Suponhamos que $e\mathcal{D}f$. Então $e\mathcal{R}a\mathcal{L}f$, para algum a, pela Proposição 1.41. Mas então $e = aa^{-1}$ e $f = a^{-1}a$. Logo, também pela Proposição 1.41, $e\mathcal{D}f$.

(2) Seja $(s, t) \in \mathcal{D}$. Então $(s^{-1}s, t^{-1}t) \in \mathcal{D}$. Por (1), existe $a \in S$ tal que $aa^{-1} = s^{-1}s$ e $a^{-1}a = t^{-1}t$. Fazendo $b = sat^{-1}$, facilmente se verifica que a e b satisfazem as propriedades, tal como, facilmente se demonstra o recíproco.

(3) O resultado é verdadeiro para $n = 2$, porque, se $a \cdot b$ é um qualquer produto restrito, então, por definição $\mathbf{d}(a) = \mathbf{r}(b)$. Assim, $a\mathcal{L}a^{-1}a = bb^{-1}\mathcal{R}b$. Logo, $a\mathcal{L}b$, pela Proposição 1.41. Mas, pelo Lema 1.72, $\mathbf{r}(a \cdot b) = \mathbf{r}(a)$. Então, $(a \cdot b, a) \in \mathcal{D}$ e $(a \cdot b, b) \in \mathcal{D}$. Para o caso de um n arbitrário, resultado sai agora naturalmente uma vez que $(a_i, a_{i+1}) \in \mathcal{D}$ para $i = 1, ..., n-1$, e $(s, a_1) \in \mathcal{D}$ □

Um semigrupo inverso contendo uma única $\mathcal{D}$- classe diz-se *bisimples*. Um semigrupo inverso com zero diz-se 0-*bisimples* se contiver exactamente duas $\mathcal{D}$- classes.

Um semigrupo inverso com zero diz-se 0-*simples* se contiver pelo menos um elemento diferente de zero e os únicos ideais são $\{0\}$ e S. Note-se que os semigrupos inversos (0-)bisimples são sempre (0-)simples.

Capítulo 2

MONOIDE BICÍCLICO E PROPRIEDADES

1 Introdução

O monoide bicíclico $\mathbf{B}$ é definido pela apresentação $\langle b, c \mid bc = 1\rangle$. Podemos pensar em $\mathbf{B}$ como sendo o conjunto natural de formas normais $\{c^i b^j : i, j \geq 0\}$, com operação:

$$c^i b^j c^k b^l = \begin{cases} c^{i-j+k} b^l & \text{caso } j \leq k \\ c^i b^{j-k+l} & \text{caso } j > k. \end{cases}$$

O monoide bicíclico é um dos semigrupos mais importantes na teoria de semigrupos. É um dos principais ingredientes das extensões de Bruck-Reilly (ver [18]), é também a base de várias generalizações; ver [1], [4], [11], [17]. O monoide bicíclico é conhecido como tendo propriedades notáveis. Por exemplo, é completamente determinado pelo seu reticulado de subsemigrupos; ver [34] e [35]. Também, como semigrupo inverso, este fica completamente determinado pelo reticulado dos subsemigrupos inversos; ver [8]. Jones [20] estuda semigrupos inversos com a seguinte propriedade: um reticulado de semigrupos contendo todos os idempotentes é distributivo. Ele mostra que o monoide bicíclico é um deles, e descreve o próprio reticulado. Finalmente, em [27] os autores estudam as propriedades de um subsemigrupo de $\mathbf{B}$ específico. Mais à frente, ainda nesta dissertação, poderemos também ver como, em [6] e [7], os autores nos descrevem os subsemigrupos de $\mathbf{B}$ e propriedades dos mesmos.

2 Propriedades

Um semigrupo inverso $FIS(X)$ equipado com a função $\iota : X \to FIS(X)$, diz-se um *semigrupo inverso livre em* X se para todo semigrupo inverso S e função $\kappa : X \to S$ existe um único homomorfismo $\theta : FIS(X) \to S$ tal que $\theta\iota = \kappa$. Uma *apresentação de semigrupo inverso* é o par (X, ρ) em que ρ é uma relação em $FIS(X)$. Um semigrupo inverso $FIS(X)/\rho^\sharp$ diz-se *apresentado* pelos *geradores* X e *relações* ρ, e denota-se por $S = Inv\langle X : \rho\rangle$. Se tanto X como ρ forem finitos, diz-se que S é *finitamente apresentado*. Um semigrupo inverso S diz-se *monogénico* se tiver uma apresentação de semigrupo inverso com um gerador.

Seja S um semigrupo inverso com uma $\mathcal{D} - classe$ cuja ordem parcial natural é não trivial. Então para cada idempotente $e \in D$ existe um idempotente $f \in D$ tal que $f < e$, pelo Teorema 1.68. Contudo, uma vez que $e\mathcal{D}f$, existe $a \in D$ tal que $a^{-1}a = e \quad \text{e} \quad aa^{-1} = f$, pela Proposição 1.73.

Vamos focar a nossa atenção no subsemigrupo inverso de S gerado por a. Note-se que este semigrupo é um monoide com identidade e, uma vez que $ea = a = ae$ e $ea^{-1} = a^{-1} = a^{-1}e$. Mostraremos que este monoide inverso é determinado unicamente por um isomorfismo pelo facto de ser gerado como monoide por a e a^{-1} e pelo facto de $a^{-1}a$ ser a identidade.

Para obtermos uma representação deste monoide, suponhamos que S é um monoide simétrico inverso. Então e será uma identidade parcial definida num conjunto isomorfo a um subconjunto próprio dele, nomeadamente o domínio de f. Tais conjuntos dizem-se *Dedekind infinitos*. Assim, o exemplo mais simples de idempotentes e e f que satisfazem as condições anteriores aparece-nos no monoide inverso simétrico $I(\mathbb{N})$; o conjunto $\mathbb{N}$ é isomorfo ao subconjunto próprio $\mathbb{N}\backslash\{0\}$ através da função sucessor $\alpha : \mathbb{N} \to \mathbb{N}$ definida por $\alpha(n) = n + 1$. A função $\alpha \in I(\mathbb{N})$, gera um submonoide inverso de $I(\mathbb{N})$ que denotamos por B. Note-se que $\alpha^{-1}\alpha = 1$ é a identidade no conjunto $\mathbb{N}$.

Defina-se agora $\theta : \mathbf{B} \to B$ de tal modo que $\theta(b) = \alpha^{-1} \quad \text{e} \quad \theta(c) = \alpha$.

Teorema 2.1. *O monoide bicíclico é isomorfo ao monoide inverso gerado pela função sucessor nos números naturais.*

Demonstração. É imediato, de $bc = 1$, que cada elemento de $\mathbf{B}$ é do tipo $c^m b^n$, para algum $m, n \in \mathbb{N}$. Suponhamos agora que $c^m b^n \equiv c^r b^s$ (equivalentes). Então $\theta(c^m b^n) = \theta(c^r b^s)$, logo, $\alpha^m\alpha^{-n} = \alpha^r\alpha^{-s}$ (considerando $\alpha^{-n} = (\alpha^{-1})^n$). Mas $(\alpha^m\alpha^{-n})(n) = m$ e portanto, $(\alpha^r\alpha^{-s})(n) = m$. Contudo,

$$(\alpha^r\alpha^{-s})(n) = (n - s) + r$$

e $0 \leq n - s$. Logo, $m - n = r - s$. De forma análoga, $(\alpha^r \alpha^{-s})(s) = r$ portanto $(\alpha^m \alpha^{-n})(s)$ está definido. Em particular, $0 \leq s - n$. Logo, $n = s$ e $m = r$, que nos dá $c^m b^n = c^r b^s$. Consequentemente, os elementos $c^m b^n$ formam uma transversal (passando por todas as classes) para as classes de congruência, e portanto formam um conjunto de formas normais. Logo, o homomorfismo entre $\mathbf{B}$ e B é injectivo, e consequentemente os semigrupos $\mathbf{B}$ e B são isomorfos.

□

A transversal obtida anteriormente pode ser usado para obter uma representação mais conveniente do monoide bicíclico. Consideremos a operação $\dot{-}$, algumas vezes chamada de *monus*, definida, no conjunto dos números naturais, do seguinte modo:

$$a \dot{-} d = \begin{cases} a - d & \text{caso } a \geq d \\ 0 & \text{caso contrário} \end{cases}$$

Defina-se, no conjunto $\mathbb{N} \times \mathbb{N}$, a operação binária

$$(m, n)(r, s) = (m + (r \dot{-} n),\ s + (n \dot{-} r)).$$

Proposição 2.2. *O monoide bicíclico é isomorfo ao conjunto* $\mathbb{N} \times \mathbb{N}$ *munido da operação binária anterior.*

Demonstração. Consideremos o produto $(c^m b^n)(c^r b^s)$.

Se $n = r$ então, $(c^m b^n)(c^r b^s) = (c^m b^s)$;

se $(n > r)$ então, $(c^m b^n)(c^r b^s) = (c^m b^{(n-r)+s})$;

se $(n < r)$ então, $(c^m b^n)(c^r b^s) = (c^{(m+(r-n))} b^s)$.

Consideremos a função $\theta : \mathbf{B} \to \mathbb{N} \times \mathbb{N}$, em que $\theta(c^m b^n) = (m, n)$. Esta função é bijectiva, e facilmente verificamos que trata de um homomorfismo das respectivas operações binárias. □

Nas propriedades seguintes vamos assumir $\mathbf{B}$ como sendo pares ordenados de números naturais.

Teorema 2.3. *O monoide bicíclico é um monoide combinatorial, bisimples, E-unitário inverso.*

Demonstração. Facilmente verificamos que os elementos idempotentes são da forma (m, m). Se (m, m) e (n, n) são idempotentes então

$$(m, m)(n, n) = (\max(m, n), \max(m, n)) = (n, n)(m, m).$$

Logo, os idempotentes formam um subsemigrupo comutativo. Para demonstrar que o monoide bicíclico é inverso, observe-se que $(m,n)(n,s) = (m,s)$, e então, $(m,n) = (m,n)(n,m)(m,n)$ para qualquer (m,n). Assim, o monoide bicíclico é regular com idempotentes comutativos, e portanto é inverso. O inverso de (m,n) é (n,m). Observe-se que

$$(m,n)^{-1}(m,n) = (n,n) \quad \text{e} \quad (m,n)(m,n)^{-1} = (m,m).$$

Logo o monoide bicíclico é combinatorial.

Se (m,m) e (n,n) forem quaisquer dois idempotentes então o elemento (m,n) satisfaz $(m,m)\mathcal{R}(m,n)$ e $(m,n)\mathcal{L}(n,n)$. Assim, $(m,m)\mathcal{D}(n,n)$, e portanto, o monoide bicíclico é bisimples.

Caracterizemos agora uma ordem parcial natural. Suponhamos que $(m,n) \leq (b,c)$. Então, $(m,n) = (b,c)(n,n)$. Por definição

$$(b,c)(n,n) = (b + (n \dot{-} b),\ n + (c \dot{-} n)).$$

Assim,

$$m = b + (n \dot{-} c) \quad \text{e} \quad n = (c \dot{-} n).$$

Mas $n = n + (c \dot{-} n)$ implica que $0 = c \dot{-} n$, e portanto $c \leq n$. Seja $a = n - c$. Logo, $m = a + b$ e $n = a + c$. Reciprocamente, supomos que $m = a + b$ e $n = a + c$, para algum número natural a. Então

$$(b,c)(n,n) = (b + (n\dot{-}c),\ n + (c\dot{-}n)) = (m,n).$$

Provamos portanto que, a ordem parcial natural é dada por:

$$(m,n) \leq (b,c) \Leftrightarrow m = a + b \quad \text{e} \quad n = a + c$$

para algum número natural a.

É agora imediato que, qualquer elemento acima de um idempotente é também um idempotente. Logo, o monoide bicíclico é E-unitário

□

Pelo Teorema 2.3, a ordem parcial natural no semireticulado de idempotentes é dado por $(m,m) \leq (n,n)$, precisamente quando $m \geq n$, que é o dual da vulgar ordenação nos números naturais. Denotamos por $(w, \leq)$, o par formado pelos números naturais sob o dual da ordem parcial. É claro que, o semireticulado de idempotentes de um monoide bicíclico é isomorfo ao semireticulado anterior. Generalizando, um *w-semigrupo inverso* é qualquer semigrupo inverso cujo semireticulado de idempotentes é isomorfo a $(w, \leq)$.

O lema seguinte é bastante interessante porque mostra como a conjugação de idempotentes pode ser usada para reaver as operações adição e monus de números naturais.

Lema 2.4. *Seja* $(a,0),(m,m) \in \mathbf{B}$.

(1) $(a,0)(m,m)(a,0)^{-1} = (a+m,\ a+m)$;

(2) $(a,0)^{-1}(m,m)(a,0) = (m \dot{-} a,\ m \dot{-} a)$.

A demonstração faz-se através do cálculo directo.

Todas as imagens homomorficas do monoide bicíclico podem ser descritas. A chave para a solução deste problema acaba por ser a *congruência do grupo mínimo*. Para termos uma noção do que se trata comecemos por introduzir algumas definições. Se ρ for uma qualquer congruência em S e S/ρ for um grupo então diz-se que ρ é uma *congruência de grupo*.

Prova-se em [26] que definindo, num semigrupo inverso S, *relação de compatibilidade* por

$$s \sim t \Leftrightarrow st^{-1}, s^{-1}t \in E(S), \forall s,t \in S.$$

e a relação σ por

$$s\ \sigma\ t \Leftrightarrow \exists u \in S : u \leq s \text{ e } u \leq t$$

temos e teorema

Teorema 2.5. *Seja S um semigrupo inverso.*

(1) *σ é e menor congruência em S contendo a relação de compatibilidade.*

(2) *S/σ é um grupo.*

(3) *Se ρ for uma qualquer congruência em S tal que S/ρ for um grupo, então $\sigma \subseteq \rho$.*

A congruência σ diz-se congruência do grupo mínimo.

Teorema 2.6. *Qualquer congruência própria no monoide bicíclico é uma congruência de grupo. Em particular, $\mathbf{B}/\sigma$ é o grupo dos inteiros.*

Demonstração. Seja ρ um congruência própria em $\mathbf{B}$. Mostremos primeiro que $(0,0)\ \rho\ (1,1)$. Como ρ é próprio, existe pelo menos dois elementos distintos

$(m,n),(b,c) \in \boldsymbol{B}$ tais que, $(m,n)\ \rho\ (b,c)$. Considerando os inversos dos elementos, caso seja necessário, podemos assumir que $m \neq b$.

Consideremos, sem perda de generalidade, $m < b$. Pela Proposição 1.69, temos $(m,m)\ \rho\ (b,b)$. Pelo Lema 2.4,

$$(0,m)(m,m)(m,0) = (0,0)$$

e

$$(0,m)(b,b)(m,0) = (b-m, b-m).$$

Assim, $(0,0)\ \rho\ (b-m,b-m)$. Seja $t = b-m$ e $0 \leq k \leq t$. Então, $(k,k) = (0,0)(k,k)$, como $(0,0)$ é a identidade e $(t,t) = (t,t)(k,k)$, da demonstração do Teorema 2.3. Desta maneira,

$$(k,k) = (0,0)(k,k)\ \rho\ (t,t)(k,k) = (t,t).$$

Tiramos que $(k,k)\ \rho\ (t,t)$, para todo $0 \leq k \leq t$. Como $t \geq 1$, temos que $(0,0)\ \rho\ (t,t)$ e $(1,1)\ \rho\ (t,t)$. Logo, $(0,0)\ \rho\ (1,1)$.

Podemos agora provar que todos os idempotentes são identificados por ρ. Para todo $k \geq 0$, temos que $(k+1,k+1) = (k,0)(1,1)(0,k)$ e $(k,k) = (k,0)(0,0)(0,k)$, pelo Lema 2.4. Assim,

$$(k+1,k+1) = (k,0)(1,1)(0,k)\ \rho\ (k,0)(0,0)(0,k) = (k,k).$$

Logo, todos os idempotentes estão ρ-relacionados com $(0,0)$. Consequentemente, cada congruência própria é uma congruência de grupo.

Caracterizemos agora a congruência do grupo mínimo; provamos que

$$(m,n)\ \sigma\ (b,c) \Leftrightarrow m-n = b-c.$$

Suponhamos que $(m,n)\ \sigma\ (b,c)$. Então, existe (e,f) tal que $(e,f) \leq (m,n)$ e $(e,f) \leq (b,c)$. Assim, existem números naturais a e d tal que

$$e = m+a, \quad f = n+a, \quad e = b+d \text{ e } f = c+d$$

da demonstração do Teorema 2.3. Logo, $m-n = e-f = b-c$.

Reciprocamente, supomos que $m-n = b-c$. Façamos $e = \max\{m,b\}$ e $f = \max\{n,c\}$. Pretendemos mostrar que $(e,f) \leq (m,n)(b,c)$. Seja $a = e-m$, que é zero se $b \leq m$ e $b-m$ caso contrário. Consideremos agora $f-n$, que é zero se $c \leq n$ e $c-n$ caso contrário. Mas como $b-m = c-n$, então, em todos os

casos, $a = e - m = f - n$. Como $e = m + a$ e $f = n + a$, então, $(e, f) \leq (m, n)$. Podemos ainda provar, de forma análoga, que $(e, f) \leq (b, c)$.

Definido $\theta : \mathbf{B} \to \mathbb{Z}$ em que $\theta(\sigma(m, n)) = m - n$, pelo resultado anterior, é uma bijecção bem definida. Também se verifica facilmente que é um homomorfismo. □

O resultado seguinte dá-nos uma apresentação de semigrupos para o monoide bicíclico.

Teorema 2.7. *O semigrupo dado pela apresentação de semigrupo seguinte*

$$S = \langle a, d : ada = a,\ dad = d,\ a = a^2d \ \ e \ \ d = ad^2 \rangle$$

é um monoide com identidade ab, que é isomorfo ao monoide bicíclico.

Demonstração. Seja $e = ad$, então, $ea = ada = a$ e $ae = a^2d = a$. De modo análogo, $ed = ad^2 = d$ e $de = dad = d$. Cada elemento de S é um produto de a's e d's. Logo, e é uma identidade (e portanto a identidade) de S. Assim, S é uma imagem isomorfa de $\langle b, c : bc = 1 \rangle$ sob o homomorfismo que aplica b em a e c em d. Consideremos a congruência induzida em $\langle b, c : bc = 1 \rangle$ por este homomorfismo. Se este for próprio, então, pelo Teorema 2.6, S será um grupo. Contudo, podemos definir um homomorfismo sobrejectivo do semigrupo livre em $\{a, d\}$ para $\mathbf{B}$, que aplica a em b e d em c. Além disso, as imagens obtidas através deste homomorfismo de cada uma das relações na apresentação de S ainda se mantém em $\mathbf{B}$. Assim, B é uma imagem isomorfa de S pela Proposição 1.70. Logo, se S for um grupo, então, também o seria $\mathbf{B}$. Assim, a congruência não pode ser própria e portanto, os semigrupos são isomorfos.

□

Vamos agora investigar o caso do semigrupo bicíclico como um subsemigrupo.

Proposição 2.8. *Seja S um semigrupo inverso. Se a $\mathcal{J}$-classe J contiver elementos x e y tais que $x < y$, então, J contém uma cópia do monoide bicíclico.*

Demonstração. De $x < y$ temos que $x^{-1}x \leq y^{-1}y$. Note-se que, se $x^{-1}x = y^{-1}y$ então teríamos $x = y$, logo, $x^{-1}x < y^{-1}y$. É óbvio que $x^{-1}x, y^{-1}y \in J$. Assim, podemos assumir, sem perda de generalidade, que x e y são idempotentes e e f tais que $e < f$ com $e, f \in J$. Como $e \mathcal{J} f$, existem $u, v \in S$ tais que $f = uev$. Fazendo $a = fue$ e $d = evf$, então,

$$ada = (fue)(evf)(fue) = f(uev)fue = fue = a$$

e

$$dad = (evf)(fue)(evf) = evf(uev)f = evf = d.$$

Logo, a e d são mutuamente inversos, e portanto ad e da são idempotentes. Note-se que

$$ad = (fue)(evf) = fuevf = f \quad \text{e} \quad da = (evf)(fue) = evfue \leq e < f$$

assim,

$$a^2b = af = aef = ae = a \quad \text{e} \quad ad^2 = fd = d$$

logo, a e d geram um subsemigrupo T de S que, pelo Teorema 2.7, é uma imagem homomorfica do monoide bicíclico. Contudo, $ad \neq da$ e portanto, este subsemigrupo é na verdade o monoide bicíclico. Pelo Teorema 2.3, o monoide bicíclico é bisimples, logo, T é um subsemigrupo de J.

□

Mais resultados importantes podem ser encontrados em [26], [34] e ainda propriedades adicionais do semigrupo bicíclico em [12], sob a forma de exercícios.

3 ω - Semigrupos inversos

Um ω-semigrupo inverso é um semigrupo inverso cujo semireticulado de idempotentes é isomorfo ao conjunto dos números naturais com o inverso da sua ordem habitual; o monoide bicíclico é um ω-semigrupo (secção anterior). Nesta secção, mostramos como a teoria de congruências split Billhart podem ser usadas para obter uma estrutura teórica para ω-semigrupos. A chave desta teoria é o monoide bicíclico.

Daremos primeiro algumas definições essenciais para a compreensão dos resultados apresentados nesta secção.

Seja $(E, \leq)$ um semireticulado, e seja T_E o conjunto de todos os isomorfismos ordenados entre os ideais principais ordenados de E. É claro que $(E, \leq)$ é um subconjunto de $I(E)$. Seguidamente apresentamos um teorema cuja demonstração é omitida.

Teorema 2.9. *O conjunto T_E é um subsemigrupo inverso de $I(E)$ cujo semireticulado de idempotentes é isomorfo a E.*

Chamamos a T_E o ***semigrupo de Munn*** do semireticulado E. O que se segue é o teorema da representação de Munn:

Teorema 2.10. *Seja S um semigrupo inverso. Então, existe um homomorfismo que separa idempotentes $\delta : S \to T_{E_{(S)}}$ tal que $\ker \delta = \mu$, em que μ é congruência idempotente de separação máxima de S, e cuja imagem é um semigrupo inverso completo de $T_{E_{(S)}}$.*

Utilizando este resultado prova-se o seguinte:

Teorema 2.11. *Seja S um semigrupo inverso. Então, S é fundamental se e só se S for isomorfo a um subsemigrupo inverso completo do semigrupo de Munn $T_{E_{(S)}}$.*

Para ver as demonstrações e saber mais sobre este assunto consultar [26, capítulo 5].

3.1 ω-semigrupos fundamentais

O monoide bicíclico é combinatorial e portanto fundamental. Assim, pelo Teorema 2.11, é isomorfo a um subsemigrupo completo do semigrupo de Munn nos seus semireticulados de idempotentes, que denotaremos por T_ω. De facto, verifica-se um resultado ainda mais forte.

Denotemos por $(w, \leq)$ o conjunto parcialmente ordenado que consiste no conjunto dos números naturais monido da ordem dual da relação de ordem usual. Temos então

Teorema 2.12. *O semigrupo de Munn T_ω é isomorfo ao monoide bicíclico.*

Demonstração. Mostraremos que T_ω é isomorfo ao conjunto $\mathbb{N} \times \mathbb{N}$ munido da operação binária definida na Proposição 2.2.

Os ideais principais ordenados de $(\omega, \leq)$ são os conjuntos da forma $[n]$ para cada $n \in \omega$. É claro que quaisquer dois ideais principais são isomorfos, além disso, existe precisamente um isomorfismo entre eles. Vamos tentar obter uma descrição explícita destes isomorfismos. Denotemos por $\theta_{m,n}$ o único isomorfismo entre $[m]$ e $[n]$. Então facilmente verificamos que

$$\theta_{m,n}(x) = x + (n - m).$$

Determinemos agora o produto $\theta_{m,n}\theta_{b,c}$. Seja $t = \max\{m, c\}$. Então

$$\mathrm{dom}(\theta_{m,n}\theta_{b,c}) = \theta_{b,c}^{-1}([t]) = [t + b - c] = [b + (m \dot{-} c)]$$

e

$$\mathrm{im}(\theta_{m,n}\theta_{b,c}) = \theta_{m,n}([t]) = [t + n - m] = [n + (c \dot{-} m)].$$

Definindo a função $\iota : T_\omega \to \mathbf{B}$ por $\iota(\theta_{m,n}) = (n, m)$, facilmente se verifica que é um isomorfismo.

□

Pelo Teorema 2.12, todo o ω-semigrupo fundamental é isomorfo a um subsemigrupo inverso completo do monoide bicíclico. Pretendemos agora obter um descrição explícita de tais subsemigrupos inversos. Para tal, necessitamos de algumas definições.

Seja m um número natural. O conjunto E_m é definido como sendo o conjunto vazio quando $m = 0$, e para $m \geq 1$ definimos

$$E_m = \{(0, 0), ..., (m - 1, m - 1)\}.$$

Logo, E_m consiste nos m idempotentes superiores do monoide bicíclico. Seja d um número natural diferente de zero. Definindo o conjunto

$$I_{(m,d)} = \{(a, b) \in \mathbf{B} : m \leq a, b \quad \text{e} \quad a \equiv b \bmod d\}.$$

Consideremos por fim

$$B_{(m,d)} = E_m \cup I_{(m,d)}$$

e

$$B_d = B_{(0,d)} = \{(a, b) \in \mathbf{B} : \ a \equiv b \bmod d\}.$$

Teorema 2.13. *$B_{(m,d)}$ é um subsemigrupo inverso completo do monoide bicíclico tal que:*

(1) *B_1 é um monoide bicíclico e bisimples;*

(2) *Para $d \geq 2$, B_d é um monoide inverso simples com d $\mathcal{D}-$classes;*

(3) *Para $m \geq 1$, $B_{(m,d)}$ é não simples tendo $I_{(m,d)}$ como ideal próprio. Além disso, $I_{(m,d)}$ é isomorfo a B_d.*

Demonstração. Por definição $B_{(m,d)} = E_m \cup I_{(m,d)}$. Mostremos primeiro que $I_{(m,d)}$ é um subsemigrupo inverso de $\mathbf{B}$. Seja $(a, b), (g, h) \in I_{(m,d)}$. Pela definição $m \leq a, b, g, h$ com $a \equiv b \mod d$ e $g \equiv h \mod d$. Também da definição

$$(a, b)(g, h) = (a + (g \dot{-} b),\ h + (b \dot{-} g)).$$

Como $m \leq a, h$ as entradas do produto são ambas maiores ou igual a m. A diferença das duas entradas é

$$a - h + ((g \dot{-} b) - (b \dot{-} g)) = (a - b) + (g - h)$$

que é divisível por d. Logo, $I_{(m,d)}$ é fechado para a multiplicação. É imediato que $I_{(m,d)}$ é fechado relativamente aos inversos e portanto $I_{(m,d)}$ é um subsemigrupo inverso. O maior idempotente em $I_{(m,d)}$ é (m,m); é claro que todos os idempotentes menores, de $\mathbf{B}$ pertencem a $I_{(m,d)}$. Os elementos de E_m são todos os idempotentes de $\mathbf{B}$ maiores do que qualquer idempotente de $I_{(m,d)}$. Logo, $B_{(m,d)}$ é um subsemigrupo inverso completo.

(1) Tiramos imediatamente do Teorema 2.3.

(2) Observe-se que quando $b \equiv g \bmod d$ temos $(a,b)\mathcal{D}(g,h)$. Logo, os idempotentes $(0,0),\ldots,(d-1,d-1)$ formam uma transversal idempotente de $\mathcal{D}-classes$. Dado um par de idempotentes (a,a) e (b,b) desta transversal podemos facilmente encontrar um número natural c tal que $c \geq b$ e $c \equiv a(\bmod d)$. Consequentemente, o semigrupo é simples porque $(a,a)\mathcal{D}(c,c) \leq (b,b)$.

(3) Os únicos elementos de $B_{(m,d)}$ que não estão contidos em $I_{(m,d)}$ são os idempotentes $(0,0),\ldots,(m-1,m-1)$, dos quais cada um deles é maior do que qualquer idempotente de $I_{(m,d)}$.

Neste momento, facilmente verificamos que $I_{(m,d)}$ é um ideal (próprio).

Definamos $\phi : I_{(m,d)} \to B_d$ por $\phi(a,b) = (a-m, b-m)$. É imediato que ϕ é uma bijecção bem definida, portanto, basta-nos provar que ϕ é um homomorfismo. Pela definição

$$\phi((a,b)(g,h)) = (a-m+(g \dot{-} b), h-m+(b \dot{-} g))$$

e

$$\phi(a,b)\phi(g,h) = (a-m+((g-m) \dot{-} (b-m)), h-m+((b-m) \dot{-} (g-m)))$$

que, pelas propriedades da operação monus, são iguais. Assim, ϕ é um homomorfismo, e portanto, um isomorfismo.

□

Provaremos no Teorema 2.15 que todo o subsemigrupo inverso completo do monoide bicíclico é da forma $B_{(m,d)}$ para algum m e d. O lema seguinte ser-nos-á útil.

Lema 2.14. *No monoide bicíclico verificam-se os seguintes resultados.*

(1) *Seja* $(a, a+d)$ *um elemento do monoide bicíclico e* $(b,b) \leq (a,a)$. *Então* $(b,b)(a,a+d)^k = (b, b+kd)$ *para todo* $k \geq 0$.

(2) *Os elementos de* $I_{(m,d)}$ *são precisamente os elementos da forma*

$$(m, m+d)^{-k}(n,n)(m,m+d)^l$$

em que $(n,n) \leq (m,m)$ *e* $0 \leq k, l$.

Demonstração.

(1) Pode-se provar por indução que $(a,a+d)^k = (a, a+kd)$ para todo $k \geq 1$, e um calculo directo mostra-nos que $(b,b)(a,a+d)^k = (b, b+kd)$ para todo $k \geq 1$. É imediato que o resultado mantém-se quando $k = 1$.

(2) Mostremos primeiro que cada elemento de $I_{(m,d)}$ é da forma $(n+kd, n+ld)$ quando $m \leq n$ e $0 \leq k, l$. Seja $(a,b) \in I_{(m,d)}$. Podemos dizer, sem perda de generalidade, que $b \leq a$. Então $a = b + qd$ para algum q, uma vez que d divide $a - b$. Por suposição, $m \leq b$, logo, $b - m = q'd + r$ para algum q' e r. Assim,

$$(a,b) = ((m+r) + (q'+q)d, (m+r) + q'd),$$

que é da forma $(n+kd, n+ld)$ quando $m \leq n$ e $0 \leq k, l$. Reciprocamente, é claro que cada elemento desta forma pertence a $I_{(m,d)}$. Por (1), temos que

$$(n+kd, n+ld) = (m, m+d)^{-k}(n,n)(m,m+d)^l$$

como pretendido.

□

Seja U um subsemigrupo inverso completo do monoide bicíclico que contém elementos não idempotentes. Consideremos

$$m_0 = \min\{m \in \mathbb{N} : (m,n) \in U \text{ para algum } n \neq m\},$$

e

$$d_0 = \min\{d \in \mathbb{N} \setminus \{0\} : (m_0, m_0 + d) \in U\}.$$

Teorema 2.15. *Seja* U *um subsemigrupo inverso completo do monoide bicíclico. Então* U *ou é um semireticulado de idempotentes ou* $U = B_{m_0,d_0}$ *para alguns* m_0 *e* d_0.

DEMONSTRAÇÃO. Suponhamos que U não é um semireticulado de idempotentes. Então, existe $(m,n) \in U$, para algum $m,n \in \mathbb{N}$, tal que $m \neq n$. Desta forma, m_0 e d_0 estão bem definidos e $(m_0,m_0)+d_0 \in U$. Supomos que U é um subsemigrupo inverso completo de $\mathbf{B}$, e portanto, em particular $(m_0,m_0) \in U$. Se $(n,n) \leq (m_0,m_0)$, então

$$(n,n)(m_0,m_0+d_0) = (n,n+kd_0) \in U$$

para todo $k \geq 0$, pelo Lema 2.14(1). Assim, pelo Lema 2.14(2), $I_{(m_0,d_0)} \subseteq U$, e portanto $B_{(m_0,d_0)} \subseteq U$, uma vez que $E_{m_0} \subseteq U$.

Para provar a inclusão contrária, consideramos $(m,n) \in U$ não idempotente. Considerando os inversos, caso seja necessário, podemos assumir que $m \leq n$. Supondo $m,n \geq m_0$. Deste modo, podemos escrever $(m,n) = (m,m+kd_0+r)$ com $0 \leq r < d_0$. Provaremos que $r = 0$. Neste momento consideremos

$$(m,m+kd_0+r)(m+kd_0,m) = (m,m+r) \in U.$$

Se $m = m_0$ então $r = 0$ e $(m,n) \in B_{(m,d)}$, assim, podemos supor que $m > m_0$. Então, $(m-1+d_0,m-1) \in U$ e portanto

$$(m-1+d_0,m-1)^{-1}(m,m+r)(m-1+d_0,m-1) = (m-1,m-1+r)$$

dado $(m-1,m-1+r) \in U$

Se $m-1 = m_0$ então $r = 0$ e $(m,n) \in B_{(m,d)}$; caso contrário usamos o argumento anterior. Finalmente, obtemos $(m_0,m_0+r) \in U$. Logo, $r = 0$, e portanto $(m,n) \in B_{(m_0,d_0)}$.

□

Os Teoremas 2.13 e 2.15 constituem uma classificação completa dos ω-semigrupos fundamentais. Para vermos alguns casos especiais basta consultar [26].

3.2 Algumas propriedades de salientar

Em [36], numa curta nota dos Vachuska, podemos ver que o semigrupo bicíclico tem P_4^*. Para compreender o que isto significa faremos uma breve introdução a este tema.

Para todo o inteiro $n > 1$, dizemos que um semigrupo S tem P_n^* se para qualquer $s_1,s_2,\ldots,s_n \in S$, existem permutações distintas $\sigma,\tau \in S_n$ (o grupo simétrico em $1,2,\ldots,n$) de tal modo que

$$s_{\sigma(1)}s_{\sigma(2)}\ldots s_{\sigma(n)} = s_{\tau(1)}s_{\tau(2)}\ldots s_{\tau(n)}.$$

Em [21], Justin e Pirillo provam que o semigrupo bicíclico B tem P_5^*, mas não P_3^*, e questionam se terá P_4^*. Em [22], testes de computador sugerem que B tem realmente P_4^*. Mais tarde os Vachuska em [36] provam essa conjectura, começando por considerar o semigrupo bicíclico na seguinte forma. Seja $N = 0, 1, 2, \ldots$, e $B = N \times N$ com a multiplicação:

$$(x_1, y_1)(x_2, y_2) = (x_1 - y_1 + \max\{y_1, x_2\}, y_2 - x_2 + \max\{y_1, x_2\}).$$

Sejam $b_1 = (x_1, y_1)$, $b_2 = (x_2, y_2)$, $b_3 = (x_3, y_3)$, e $b_4 = (x_4, y_4)$, elementos de B. Para qualquer $\sigma \in S_4$, definimos os inteiros $x(\sigma)$ e $y(\sigma)$ por $b_{\sigma(1)}b_{\sigma(2)}b_{\sigma(3)}b_{\sigma(4)} = (x(\sigma), y(\sigma))$. Então, considerada como permutação de $b_i's$, $b_{\sigma(1)}b_{\sigma(2)}b_{\sigma(3)}b_{\sigma(4)}$ diz-se *extrema* se $x(\sigma) = x_{\sigma(1)}$ ou $y(\sigma) = y_{\sigma(4)}$.

Lema 2.16. *Para qualquer* $\{b_i = (x_i, y_i)\}_{i=1}^4 \subset B$, *pelo menos uma das três permutações* $b_1b_2b_3b_4$, $b_2b_3b_4b_1$, $b_4b_1b_2b_3$ *é extrema.*

Demonstração. Tem que se verificar um dos seguintes oito casos

(1) $y_1 \geq x_2,\ y_2 \geq x_3,\ y_3 \geq x_4 :\ b_1b_2b_3b_4$ é extrema.

(2) $y_1 \geq x_2,\ y_2 \geq x_3,\ y_3 \leq x_4 :\ b_1b_2b_3b_4$ é extrema.

(3) $y_1 \geq x_2,\ y_2 \leq x_3,\ y_3 \geq x_4 :\ b_1b_2b_3b_4$ ou $b_4b_1b_2b_3$ é extrema.

(4) $y_1 \geq x_2,\ y_2 \leq x_3,\ y_3 \leq x_4 :\ b_1b_2b_3b_4$ é extrema.

(5) $y_1 \leq x_2,\ y_2 \geq x_3,\ y_3 \geq x_4 :\ b_2b_3b_4b_1$ é extrema.

(6) $y_1 \leq x_2,\ y_2 \leq x_3,\ y_3 \leq x_4 :\ b_1b_2b_3b_4$ é extrema.

(7) $y_1 \leq x_2,\ y_2 \leq x_3,\ y_3 \geq x_4 :\ b_4b_1b_2b_3$ é extrema.

(8) $y_1 \leq x_2,\ y_2 \geq x_3,\ y_3 \leq x_4 :\ b_1b_2b_3b_4$ ou $b_2b_3b_4b_1$ é extrema.

Por exemplo, no caso (3), temos

$$\begin{aligned} b_1b_2b_3b_4 &= (x_1, y_1)(x_2, y_2)(x_3, y_3)(x_4, y_4) \\ &= (x_1, y_2 + y_1 - x_2)(x_3, y_4 + y_3 - x_4) \end{aligned}$$

caso não seja extrema, implica $y_2 + y_1 - x_2 < x_3$. Neste caso,

$$\begin{aligned} b_4b_1b_2b_3 &= (x_4, y_4)(x_1, y_1)(x_2, y_2)(x_3, y_3) \\ &= (x_4, y_4)(x_1, y_2 + y_1 - x_2)(x_3, y_3) \\ &= (x_4, y_4)(x_1 + x_3 - y_2 - y_1 + x_2, y_3), \end{aligned}$$

logo, tem que ser extrema.

□

Proposição 2.17. *O semigrupo bicíclico B tem P_4^*.*

DEMONSTRAÇÃO. Seja $\{b_i = (x_i, y_i)\}_{i=1}^4 \subset B$. Aplicando as 24 permutações de S_4 a $\{b_1, b_2, b_3, b_4\}$ produzimos seis conjuntos de quatro permutações, cada conjunto similar a $\{b_1b_2b_3b_4, b_2b_3b_4b_1, b_3b_4b_1b_2, b_4b_1b_2b_3\}$. Aplicando o Lema 2.16 a cada uma das permutações $b_1b_2b_3b_4$, $b_2b_3b_4b_1$, $b_3b_4b_1b_2$, e $b_4b_1b_2b_3$, observamos que pelo menos duas têm que ser extremas. Consequentemente, pelo menos 12 das 24 permutações de S_4 produzem permutações extremas de $\{b_i\}_{i=1}^4$.

Seja $\sigma \in S_4$. Se $x_{\sigma(1)} = x(\sigma)$, então

$$y(\sigma) = \sum_{i=1}^{4} y_i - \sum_{i=1}^{4} x_i + x_{\sigma(1)}.$$

Assim, existem, no máximo, quatro pares distintos no conjunto

$$\{(x(\sigma), y(\sigma)) : \sigma \in S_4, \quad x(\sigma) = x_{\sigma(1)}\}$$

uma vez que existem, no máximo, quatro possibilidades diferentes para $x_{\sigma(1)}$. De forma análoga, existem, no máximo, quatro pares distintos no conjunto

$$\{(x(\sigma), y(\sigma)) : \sigma \in S_4, \quad x(\sigma) = x_{\sigma(4)}\}.$$

Portanto, o conjunto

$$\{(x(\sigma), y(\sigma)) : \sigma \in S_4, \quad b_{\sigma(1)}b_{\sigma(2)}b_{\sigma(3)}b_{\sigma(4)} \text{ é extrema}\}$$

contém no máximo oito pares distintos. Logo, duas das 12 ou mais permutações de S_4 produzindo permutações extremas dos b_i's, devem produzir o mesmo produto.

□

Encontramos ainda em [10] uma outra propriedade, do semigrupo bicíclico, de salientar. Goralcik considera o monoide $\mathcal{M} = (\mathcal{X}, e, \cdot)$, conjunto $\mathcal{X}$ com uma multiplicação associativa e com o elemento identidade e, e define *translação esquerda* f_a,

$$f_a(x) = a \cdot x, \ \forall x \in \mathcal{X}$$

Tal elemento $a \in \mathcal{X}$ chamamos *elemento determinante esquerdo* e à sua translação esquerda f_a *translação determinante esquerda* de $\mathcal{M}$.

Goralcik diz-nos que qualquer monoide monogénico $\langle a \rangle$ é um exemplo de um monoide comutativo que tem elemento determinante simultaneamente direito e esquerdo - apenas o gerador a, neste caso. Impõe-se uma questão: Será que existe algum monoide não comutativo possuidor de elemento determinante (simultaneamente direito e esquerdo)?

Chamemos a estes monóides, *monóides não-comutativos(1,1).* Goralcik considera o semigrupo bicíclico $B = \langle b, c \rangle$, um monoide não-comutativo(1,1), com identidade e, e os dois geradores b, c satisfazendo a relação

$$bc = e,$$

e afirma que

Teorema 2.18. *Existem precisamente dois monóides não-comutativos(1,1): o semigrupo bicíclico B e B^0 (B com zero agregado).*

Identifica ainda B com o conjunto $\mathbb{N} \times \mathbb{N}$ de todos os pares ordenados (m, n), inteiros não negativos, munido da multiplicação

$$(m,n)(r,s) = \begin{cases} (r, s-m+n), & \text{caso } s \geq m, \\ (r+m-s, n) & \text{caso } s < m. \end{cases}$$

Considera ainda translação esquerda, que usa na demonstração do teorema anterior, como sendo $f_b(r,s) = b(r,s)$, para todo $(r,s) \in \mathbb{N} \times \mathbb{N}$.

Fazendo $b = (1,0)$, $c = (0,1)$, $e = (0,0)$ a translação esquerda tem a forma

$$f_b(r,s) = (1,0)(r,s) = \begin{cases} (r, s-1), & \text{caso } s \geq 1, \\ (r+1, 0) & \text{caso } s = 0. \end{cases}$$

Para uma descrição, e demonstração, mais exaustiva desta propriedade consultar [10].

4 Aplicações do Monoide bicíclico

- Uma das mais recentes aplicações do monoide bicíclico é na teoria de Anéis. Jacobson [19] investigou os aneis R contendo elementos $b, c \in R$ tais que $bc = 1$ e $cb \neq 1$. Ou seja, considerou aneis com o monoide bicíclico "embeded" no monoide multiplicativo do anel. Os idempotentes do monoide bicíclico são da forma $c^i b^i$, com $i \in \mathbb{N}$. Definindo

$$e_{i,j} = c^{i-1} b^{j-1} - c^i b^j$$

  para todos os números naturais i e j, pode-se mostrar que nenhum dos $e_{i,j}$ é zero e que o conjunto de todos $e_{i,j}$ com o zero formam um subsemigrupo de R isomorfo a $B_{\aleph_0}$. Isto tem consequências importantes para a estrutura do anel R.

- Outra aplicação importante do monoide bicíclico é na Teoria de linguagens formais. Consideremos $\Sigma = \{(,)\}$, e seja L a linguagem sobre Σ, constituída por todas as palavras em que os parêntesis estão colocados correctamente. Então o monoide sintáctico de L é o monoide bicíclico, ver [24].

- Uma última aplicação vem de λ-calculus. Hofmann e Mislove [15] e [16] mostram que qualquer imagem homomorfa do monoide bicíclico num semigrupo topológico compacto é um grupo; isto é intuitivamente plausível, porque compacto é uma condição de finitude e as únicas imagens finitas do monoide bicíclico são os grupos. Eles usaram o seu resultado para investigar a existência de certos modelos de λ-calculus.

Capítulo 3

SUBSEMIGRUPOS DO MONOIDE BICÍCLICO

Neste capítulo fazemos a descrição de todos os subsemigrupos do monoide bicíclico **B**. Mostramos que existem essencialmente cinco diferentes tipos de subsemigrupos. Cada subsemigrupo é caracterizado por uma certa colecção de parâmetros. Determinamos os subsemigrupos regulares, simples e bisimples de **B**. Apresentamos algoritmos para obter os parâmetros a partir do conjunto gerador; ver [6]. Estudamos também algumas das propriedades dos subsemigrupos do monoide bicíclico **B**. Apresentamos condições necessárias e suficientes para que um subsemigrupo seja finitamente gerado, automático e finitamente apresentado. Finalmente, demonstramos que um subsemigrupo de **B** é residualmente finito se e só se não contiver uma cópia de **B**; ver [7].

1 Introdução

Neste capítulo daremos a descrição de todos os subsemigrupos de **B**. Mostraremos que existem essencialmente cinco diferentes tipos de subsemigrupos. Um deles é o caso degenerado de subconjuntos de $\{c^i b^j : i, j \geq 0\}$, e os seguintes quatro dividem-se em dois grupos de dois, ligados pelo óbvio anti-isomorfismo de **B** $\widehat{\ }: c^i b^j \mapsto c^j b^i$. A nossa descrição sobre os quatro tipos de subsemigrupos não pertencentes à classe dos não degenerados é puramente técnica, e depende de uma colecção de parâmetros. Não constitui um classificação completa dos subsemigrupos, pois não temos um conjunto de condições que nos digam que escolhas de parâmetros produzem subsemigrupos ou não. Numa tentativa de obter tal classificação temos que enfrentar o facto

de que $\mathbf{B}$ contem copias do semigrupo aditivo de números naturais $\mathbb{N}$, cujos subsemigrupos estão muito longe de serem completamente entendidos; ver [32, Cap.10], [35] e algumas citações aí feitas. É mais realista desejar reduzir a classificação dos subsemigrupos de $\mathbf{B}$ à classificação dos subsemigrupos de $\mathbb{N}$.

Apresentamos aqui um conjunto de algoritmos que determina os parâmetros, a partir de um conjunto de geradores, e que pode ser aplicado para verificar se a colecção de parâmetros define ou não um subsemigrupo.

Na secção 2 definimos um série de subconjuntos de $\mathbf{B}$ notáveis, que serão usados posteriormente como um género de construção em blocos, depois apresentaremos o nosso principal teorema na secção 3. A secção 4 contém resultados auxiliares necessários para provar o teorema principal (apresentado na secção anterior). Nas secções 5 e 6 respectivamente consideramos dois tipos de subsemigrupos não degenerados. Na secção 7, determinamos, usando a nossa descrição, os subsemigrupos regulares de $\mathbf{B}$, os simples e os bisimples. Finalmente, a secção 8 contém algoritmos para o cálculo de parâmetros.

2 Subconjuntos Notáveis

Nesta secção introduzimos a notação que usaremos nas secções seguintes. Para definirmos subconjuntos do monoide bicíclico achamos conveniente representar $\mathbf{B}$ como uma grelha quadrada infinita, tal como na Figura 3.1. Começamos por definir as funções $\Phi, \Psi, \lambda : \mathbf{B} \to \mathbb{N}_0$ como $\Phi(c^i b^j) = i$, $\Psi(c^i b^j) = j$ e $\lambda(c^i b^j) = |j - i|$, e por introduzir também alguns dos subconjuntos básicos de $\mathbf{B}$:

$D = \{c^i b^i : i \geq 0\}$ – a *diagonal* ,
$U = \{c^i b^j : j > i \geq 0\}$ – a *metade superior*,
$R_p = \{c^i b^j : j \geq p, i \geq 0\}$ – a *metade direita do plano (determinada por p)*,
$L_p = \{c^i b^j : 0 \leq j < p, i \geq 0\}$ – a *metade esquerda do plano (determinada por p)*,
$M_d = \{c^i b^j : d \mid j - i; i, j \geq 0\}$ – os λ-*multiplos de d*,

para $p \geq 0$ e $d > 0$.

Definimos agora a função $\widehat{\ }: \mathbf{B} \to \mathbf{B}$ por $c^i b^j \mapsto \widehat{c^i b^j} c^j b^i$. Geometricamente $\widehat{\ }$ é a reflexão relativamente à diagonal principal. Portanto, por exemplo, $\widehat{U}$ é a metade inferior. Algebricamente, esta função é um anti-isomorfismo ($\widehat{xy} = \widehat{y}\widehat{x}$), o que se verifica facilmente.

Usando os conjuntos e funções definidos anteriormente podemos definir agora mais alguns subconjuntos de $\mathbf{B}$ que serão usados na nossa descrição. Para $0 \leq q \leq p \leq m$ definimos o *triângulo*

	0	1	2	3	
0	1	b	b^2	b^3	$\cdots$
1	c	cb	cb^2	cb^3	$\cdots$
2	c^2	c^2b	c^2b^2	c^2b^3	$\cdots$
3	c^3	c^3b	c^3b^2	c^3b^3	$\cdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Figura 3.1: O Monoide Bicíclico

$$T_{q,p} = L_p \cap \widehat{R_q} \cap (U \cup D) = \{c^i b^j : q \leq i \leq j < p\},$$

e as *faixas*

$$\begin{aligned} S_{q,p} &= R_p \cap \widehat{R_q} \cap \widehat{L_p} = \{c^i b^j : q \leq i < p, j \geq p\}, \\ S'_{q,p} &= S_{q,p} \cup T_{q,p} = \{c^i b^j : q \leq i < p, j \geq i\}, \\ S_{q,p,m} &= S_{q,p} \cap R_m = \{c^i b^j : q \leq i < p, j \geq m\}. \end{aligned}$$

Note-se que se $q = p$ os conjuntos anteriores são vazios. Para $i, m \geq 0$ e $d > 0$ definimos as *linhas*

$$\begin{aligned} \Lambda_i &= \widehat{R_i} \cap \widehat{L_{i+1}} = \{c^i b^j : j \geq 0\}, \\ \Lambda_{i,m,d} &= \Lambda_i \cap R_m \cap M_d = \{c^i b^j : d \mid j - i, j \geq m\} \end{aligned}$$

generalizando, para $I \subseteq \{0, \ldots, m-1\}$,

$$\Lambda_{I,m,d} = \textstyle\bigcup_{i \in I} \Lambda_{i,m,d} = \{c^i b^j : i \in I, d \mid j - i, j \geq m\}.$$

Para $p \geq 0$, $d > 0$, $r \in [d] = \{0, \ldots, d-1\}$ e $P \subseteq [d]$ definimos as *grelhas*

$$\begin{aligned} \Sigma_p &= R_p \cup \widehat{R_p} = \{c^i b^j : i, j \geq p\}, \\ \Sigma_{p,d,r} &= \Sigma_p \cap \left(\bigcup_{u=0}^{\infty} \Lambda_{p+r+ud} \right) \cap \left(\bigcup_{u=0}^{\infty} \widehat{\Lambda_{p+r+ud}} \right) = \{c^{p+r+ud} b^{p+r+vd} : u, v \geq 0\}, \\ \Sigma_{p,d,P} &= \bigcup_{r \in P} \Sigma_{p,d,r} = \{c^{p+r+ud} b^{p+r+vd} : r \in P; u, v \geq 0\}. \end{aligned}$$

Alguns dos nossos subconjuntos estão ilustrados nas figuras seguintes.

Finalmente, para $X \subseteq S$, definimos $\iota(X) = \min(\Phi(X \cap U))$ (caso $X \cap U \neq \emptyset$) e $\kappa(X) = \min(\Psi(X \cap \widehat{U}))$ (caso $X \cap \widehat{U} \neq \emptyset$).

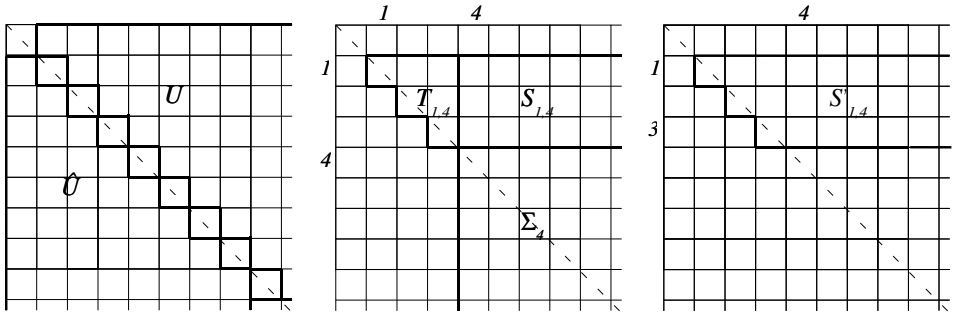


Figura 3.2: Metade superior e inferior U, $\widehat{U}$, o triângulo $T_{1,4}$ e as faixas $S_{1,4}$, $S'_{1,4}$.

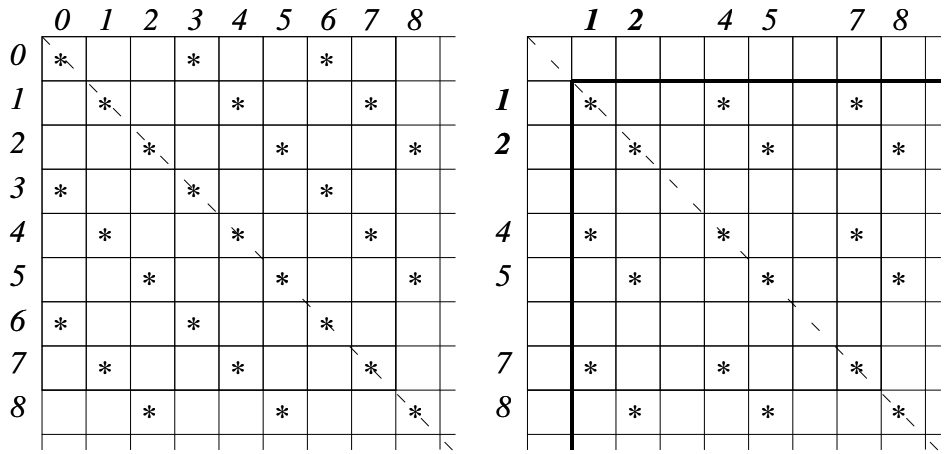


Figura 3.3: Os λ-múltiplos de 3, M_3, e a grelha $\Sigma_{1,3,\{0,1\}}$

3 Teorema Principal

Nesta secção surge-nos o *Teorema Principal* que será demonstrado nas secções seguintes.

Teorema 3.1. *Seja S um subsemigrupo de um monoide bicíclico. Então verifica-se uma das seguintes condições:*

(1) *O subsemigrupo S é um subconjunto da diagonal, isto é, $S \subseteq D$;*

(2) *O subsemigrupo S é a reunião de um subconjunto de um triângulo, um subconjunto da diagonal acima do triângulo, uma grelha abaixo do triângulo e algumas linhas pertencentes a uma faixa determinada pela grelha e o triângulo, ou a reflexão, relativamente à diagonal, desta reunião. Formalmente, existe $q, p \in \mathbb{N}_0$ com $q \leq p$, $d \in \mathbb{N}$, $I \subseteq \{q, \ldots, p-1\}$ com $q \in I$, $P \subseteq \{0, \ldots, d-1\}$ com*

$0 \in P, \quad F_D \subseteq D \cap L_q, \quad F \subseteq T_{q,p}$, *de tal modo que* S *é uma das seguintes formas:*

(i) $S = F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$;

(ii) $S = F_D \cup \widehat{F} \cup \widehat{\Lambda_{I,p,d}} \cup \Sigma_{p,d,P}$.

(3) *Existem* $d \in \mathbb{N}, \quad I \subseteq \mathbb{N}_0, \quad F_D \subseteq D \cap L_{\min(I)}$, *e conjuntos* $S_i \subseteq \Lambda_{i,i,d}$ $(i \in I)$ *tais que* S *assume uma das seguintes formas:*

(i) $S = F_D \cup \bigcup_{i \in I} S_i$;

(ii) $S = F_D \cup \bigcup_{i \in I} \widehat{S}_i$;

em que cada S_i *tem a forma*

$$S_i = F_i \cup \Lambda_{i,m_i,d}$$

para algum $m_i \in \mathbb{N}_0$, *algum conjunto finito* F_i, *e*

$$I = I_0 \cup \{r + ud : r \in R, u \in \mathbb{N}_0, r + ud \geq N\}$$

para algum $R \subseteq \{0, \ldots, d-1\}$ *(possivelmente vazio), algum* $N \in \mathbb{N}_0$ *e algum conjunto finito* $I_0 \subseteq \{0, \ldots, N-1\}$.

Comecemos por observar que se $S \subseteq D$ então não há nada a descrever uma vez que qualquer idempotente $c^i b^i$ é uma identidade para a grelha Σ_i abaixo deste.

A condição (2) corresponde a subsemigrupos com elementos acima e abaixo da diagonal; chamamos-lhe *subsemigrupos bilaterais*. Note-se que o subsemigrupo definido na condição (2)(ii) é simétrico, relativamente à diagonal, ao subsemigrupo correspondente dado na condição (2)(i), e portanto podemos o anti-isomorfismo $\widehat{\ }$ para obter um a partir do outro. Assim, basta-nos considerar subsemigrupos que caem numa destas categorias. A descrição dos subsemigrupos bilaterais é feita na secção 5.

Chamamos *subsemigrupos superiores* àqueles cujos elementos se encontram acima da diagonal, *subsemigrupos inferiores* aos que têm os elementos abaixo da diagonal. Mais uma vez as condições (3)(i) e (3)(ii) dão-nos subsemigrupos simétricos relativamente à diagonal e portanto iremos considerar apenas uma delas. O tratamento dos subsemigrupos superiores é feito na secção 6.

4 Resultados Auxiliares

Nesta secção demonstraremos algumas das propriedades dos subconjuntos definidos na secção 2.

Lema 3.2. *Para cada $d \in \mathbb{N}$, M_d (os λ-múltiplos de d) é um subsemigrupo.*

DEMONSTRAÇÃO. Sejam $c^i b^j, c^k b^l \in M_d$. Então $d \mid i-j$ e $d \mid k-l$. Se $j > k$ então $c^i b^j c^k b^l = c^i b^{j-k+l}$, caso contrário, $c^i b^j c^k b^l = c^{i-j+k} b^l$. Em qualquer um do casos $c^i b^j c^k b^l \in M_d$ porque $d \mid i-j+k-l$. □

Lema 3.3. *Para cada $p \in \mathbb{N}$, a metade direita do plano R_p e a faixa $S'_{0,p}$ são subsemigrupos.*

DEMONSTRAÇÃO. Seja $x = c^i b^j$, $y = c^k b^l \in R_p$ $(j, l \geq p)$. Se $j \geq k$ então $xy = c^i b^{j-k+l} \in R_p$ uma vez que $j-k+l \geq l \geq p$. Se $j < k$ então $xy = c^{i-j+k} b^l \in R_p$ uma vez que $l \geq p$. Portanto, R_p é um subsemigrupo. Seja $x = c^i b^j$, $y = c^k b^l \in S'_{0,p}$ $(i, k < p, j \geq i, l \geq k)$. Se $j \geq k$ então $xy = c^i b^{j-k+l} \in S'_{0,p}$ uma vez que $i < p$ e $j-k+l \geq j \geq i$. Se $j < k$ então $xy = c^{i-j+k} b^l \in S'_{0,p}$ tendo em conta que $i-j+k \leq k < p$ e $l \geq k \geq i-j+k$. Portanto, $S'_{0,p}$ é também um semigrupo. □

No resultado seguinte usaremos o facto de que a imagem de um subsemigrupo por um anti-isomorfismo é ainda um subsemigrupo.

Lema 3.4. *Para cada $d, p, m \in \mathbb{N}_0$, com $q < p \leq m$ os conjuntos seguintes são subsemigrupos:*

(i) $S_{q,p}$;	*(ii)* $S'_{q,p}$;	*(iii)* Σ_p;
(iv) $S_{q,p} \cup \Sigma_p$;	*(v)* $S_{q,p,m}$;	*(vi)* $S'_{q,p} \cup \Sigma_p$.

DEMONSTRAÇÃO. Para demonstrarmos de (i) a (v) escreveremos simplesmente os conjuntos como intersecções dos subsemigrupos dados no lema anterior e as suas imagens através do anti-isomorfismo $\widehat{\ }$. Temos que

$$S_{q,p} = S'_{0,p} \cap \widehat{R_q} \cap R_p, \quad S'_{q,p} = S'_{0,p} \cap \widehat{R_q}, \quad \Sigma_p = R_p \cap \widehat{R_p}, \quad S_{q,p} \cup \Sigma_p = R_p \cap \widehat{R_q}$$

e ainda que

$$S_{q,p,m} = S'_{0,p} \cap R_m \cap \widehat{R_q}.$$

Para provarmos que $S = S'_{q,p} \cup \Sigma_p$ é um subsemigrupo basta mostrar que, para $x = c^i b^j \in S'_{q,p}$ $(q \leq i < p, j \geq i)$ e $y = c^k b^l \in \Sigma_p$ $(k, l \geq p)$, temos $xy, yx \in S$. Se $j \geq k$ então $xy = c^i b^{j-k+l} \in S$, porque $i \geq q$ e $j-k+l \geq l \geq p$. Se $j < k$ então $xy = c^{i-j+k} b^l \in S$, porque $i-j+k > i \geq q$ e $l \geq p$. Tendo em conta que $l \geq p > i$ temos que $yx = c^k b^{l-i+j} \in \Sigma_p$, porque $k \geq p$ e $l-i+j \geq l \geq p$. □

No lema seguinte estabelecemos algumas inclusões que nos virão a ser bastante úteis.

Lema 3.5. *Para cada $p, q \in \mathbb{N}_0$, com $q < p$, verificam-se as seguintes inclusões*

$$(i)\ \ T_{q,p}S_{q,p} \subseteq S_{q,p}; \qquad (ii)\ \ S_{q,p}T_{q,p} \subseteq S_{q,p};$$
$$(iii)\ \ T_{q,p}\Sigma_p \subseteq S_{q,p} \cup \Sigma_p; \qquad (iv)\ \ \Sigma_p T_{q,p} \subseteq \Sigma_p.$$

Demonstração. Seja $\alpha = c^i b^j \in T_{q,p}$ $(q \leq i \leq j < p)$, $\beta = c^k b^l \in S_{q,p}$ $(q \leq k < p, l \geq p)$ e $\gamma = c^u b^v \in \Sigma_p$ $(u, v \geq p)$. Se $j \geq k$ então $\alpha\beta = c^i b^{j-k+l}$ e, uma vez que $j - k + l \geq l \geq p$, $\alpha\beta \in S_{q,p}$. Se $j < k$ então $\alpha\beta = c^{i-j+k} b^l$ e, uma vez que $l \geq p$ e $S'_{q,p}$ é um subsemigrupo, $\alpha\beta \in S_{q,p}$. Assim, provámos (i).

Temos que $\beta\alpha = c^k b^{l-i+j}$ uma vez que $i < p \leq l$. Tendo em conta que $l - i + j \geq l \geq p$ então $\beta\alpha \in S_{q,p}$, e assim provámos (ii).

Sabemos que $\alpha\gamma = c^{i-j+u} b^v$ porque $j < p \leq u$ e, como $v \geq p$ e $S'_{q,p} \cup \Sigma_p$ é um subsemigrupo, $\alpha\gamma \in S_{q,p} \cup \Sigma_p$. Provámos (iii).

Finalmente, como $i < p \leq v$ então $\gamma\alpha = c^u b^{v+j-i}$. Logo, $\gamma\alpha \in \Sigma_p$ porque $u \geq p$, e (iv) fica também provado. □

Lema 3.6. *Para cada $p \in \mathbb{N}_0$, $d \in \mathbb{N}$ e $P \subseteq \{0, \ldots, d-1\}$, a grelha $\Sigma_{p,d,P}$ é um subsemigrupo.*

Demonstração. Seja

$$\alpha = c^{p+r_1+u_1 d} b^{p+r_1+v_1 d}, \quad \beta = c^{p+r_2+u_2 d} b^{p+r_2+v_2 d} \in \Sigma_{p,d,P}$$

em que $r_1, r_2 \in P$; $u_1, v_1, u_2, v_2 \in \mathbb{N}_0$.

Se $p + r_1 + v_1 d \geq p + r_2 + u_2 d$ então $\alpha\beta = c^{p+r_1+u_1 d} b^{p+r_1+(v_1-u_2+v_2)d}$. Uma vez que $p + r_1 + v_1 d \geq p + r_2 + u_2 d$, segue-se que $r_1 + v_1 d - u_2 d \geq r_2 \geq 0$, o que implica $r_1 + (v_1 - u_2 + v_2)d \geq 0$. Assim temos que $(v_1 - u_2 + v_2)d \geq -r_1 > -d$, logo, $v_1 + v_2 - u_2 \geq 0$. Portanto $\alpha\beta \in \Sigma_{p,d,P}$. Se $p + r_1 + v_1 d < p + r_2 + u_2 d$ então $\alpha\beta = c^{p+r_2+(u_1-v_1+u_2)d} b^{p+r_2+v_2 d}$. Analogamente $p + r_2 + u_2 d > p + r_1 + v_1 d$ implica $u_1 - v_1 + u_2 \geq 0$ e portanto $\alpha\beta \in \Sigma_{p,d,P}$. □

Lema 3.7. *Para cada $p, q \in \mathbb{N}_0$, com $q \leq p$, $d \in \mathbb{N}$ e $P \subseteq \{0, \ldots, d-1\}$, o conjunto*

$$\Sigma_{p,d,P} \cup (M_d \cap S'_{q,p})$$

é um subsemigrupo.

DEMONSTRAÇÃO. Seja $H = \Sigma_{p,d,P} \cup (M_d \cap S'_{q,p})$. Sabemos do lema anterior que $\Sigma_{p,d,P}$ é um subsemigrupo. Dos lemas 3.2 e 3.4 sabemos que $M_d \cap S'_{q,p}$ é também um subsemigrupo. Seja $\alpha = c^{p+r+ud}b^{p+r+vd} \in \Sigma_{p,d,P}$ e $\beta = c^i b^{i+sd} \in M_d \cap S'_{q,p}$. Apenas temos que mostrar que $\alpha\beta, \beta\alpha \in H$.

Uma vez que $p + r + vd \geq p > i$, $\alpha\beta = c^{p+r+ud}b^{p+r+(v+s)d} \in \Sigma_{p,d,P}$, temos $\beta\alpha = c^i b^{i+sd}c^{p+r+ud}b^{p+r+vd}$. Note-se que $H \subseteq U = (\Sigma_p \cup S'_{q,p}) \cap M_d$ e, usando os mesmos dois lemas, U é um subsemigrupo. Portanto, se $i + sd \geq p + r + ud$ então $\beta\alpha \notin \Sigma_p$ e, como U é um subsemigrupo, $\beta\alpha \in S'_{q,p} \cap M_d \subseteq H$. Se $i + sd < p + r + ud$ e $u - s < 0$ temos novamente $\beta\alpha \in S'_{q,p} \cap M_d \subseteq H$. Finalmente, se $i+sd < p+r+ud$ e $u-s \geq 0$ então $\beta\alpha = c^{p+r+(u-s)d}b^{p+r+vd} \in \Sigma_{p,d,P}$. □

Lema 3.8. *Para cada $p \in \mathbb{N}_0$, $d \in \mathbb{N}$ e $I \subseteq \{0, \ldots, p-1\}$, o conjunto $\Lambda_{I,p,d}$ é um subsemigrupo.*

DEMONSTRAÇÃO. Sejam $\alpha = c^i b^{i+ud}$, $\beta = c^j b^{j+vd} \in \Lambda_{I,p,d}$ $(i, j < p;\ i+ud, j+vd \geq p)$. Então $\alpha\beta = c^i b^{i+(u+v)d}$ porque $i + ud \geq p > j$. Uma vez que $i + (u + v)d \geq i + ud \geq p$ obtemos $\alpha\beta \in \Lambda_{I,p,d}$. □

Lema 3.9. *Seja $p \in \mathbb{N}_0$, $d \in \mathbb{N}$, $\emptyset \neq I \subseteq \{0, \ldots, p-1\}$, $\emptyset \neq P \subseteq \{0, \ldots, d-1\}$, e $q = \min(I)$. O conjunto $H = \Sigma_{p,d,P} \cup \Lambda_{I,p,d}$ é um subsemigrupo se e só se*

$$I' = \{p + r - ud : r \in P, u \in \mathbb{N}_0, p + r - ud \geq q\} \subseteq I.$$

DEMONSTRAÇÃO. Suponhamos que H é um subsemigrupo e provemos que $I' \subseteq I$. Sejam $c^q b^{q+d_1}, c^{p+r+d}b^{p+r} \in H$ em que $r \in P$ e $d_1 > 0$ é um múltiplo de d. Para quaisquer $n, m \in \mathbb{N}$, tais que $p+r+md-nd_1 \geq q$, temos $(c^q b^{q+d_1})^n (c^{p+r+d}b^{p+r})^m = c^{p+r+md-nd_1}b^{p+r} \in H$ e portanto $p + r - ud \in I$ para qualquer $r \in P$ e $u \in \mathbb{N}$ tais que $p + r - ud \geq q$. Logo, $I' \subseteq I$.

Suponhamos agora que $I' \subseteq I$ e provemos que H é um subsemigrupo. Sabemos que $\Sigma_{p,d,P}$ é um subsemigrupo. Seja $\alpha = c^{p+r+ud}b^{p+r+vd} \in \Sigma_{p,d,P}$ $(r \in P; u, v \in \mathbb{N}_0)$ e $\beta = c^i b^{i+d_1} \in \Lambda_{I,p,d}$ $(i \in I, d_1 \in \mathbb{N}, d \mid d_1)$. Temos que $\alpha\beta = c^{p+r+ud}b^{p+r+vd+d_1} \in \Sigma_{p,d,P}$. Caso $i + d_1 \geq p + r + ud$ então $\beta\alpha = c^i b^{i+d_1+(v-u)d} \in \Lambda_{I,p,d}$, porque $i+d_1+(v-u)d \geq p+r+vd \geq p$. Se $i+d_1 < p+r+ud$ então $\beta\alpha = c^{p+r+ud-d_1}b^{p+r+vd}$. Neste caso, se $ud - d_1 \geq 0$ então $\beta\alpha \in \Sigma_{p,d,P}$ e se $ud - d_1 < 0$ logo, $p + r + ud - d_1 \geq q$ uma vez que $H \subseteq S_{q,p} \cup \Sigma_p$ e $S_{q,p} \cup \Sigma_p$ é um subsemigrupo. Portanto, $p + r + ud - d_1 \in I' \subseteq I$, o que implica $\beta\alpha \in \Lambda_{I,p,d}$. □

5 Subsemigrupos Bilaterais

Nesta secção descrevemos os subsemigrupos com elementos acima e abaixo da diagonal. Seja S um subsemigrupo de $\mathbf{B}$ com $S \cap U \neq \emptyset$ e $S \cap \widehat{U} \neq \emptyset$. Sem perda de generalidade podemos assumir que $q = \iota(S) \leq \kappa(S) = p$. Note-se que o outro caso é dual deste, basta usar a anti-isomorfismo$\widehat{\ }$.

O resultado seguinte é o mais importante desta secção:

Teorema 3.10. *Seja S é um subsemigrupo de $\boldsymbol{B}$ tal que $S \cap U \neq \emptyset$, $S \cap \widehat{U} \neq \emptyset$ e $q = \iota(S) \leq \kappa(S) = p$. Existem $d \in \mathbb{N}$, $F_D \subseteq D \cap L_q$, $F \subseteq T_{q,p}$, $I \subseteq \{q, \ldots, p-1\}$, $P \subseteq \{0, \ldots, d-1\}$ com $0 \in P$ tais que*

$$S = F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}.$$

A restante secção é dedicada à demonstração do Teorema 3.10. A prova segue a estratégia seguinte: A aplicação $\nu : \mathbf{B} \to \mathbb{Z}$ (o grupo aditivo dos inteiros), definida por $\nu(c^i b^j) = i - j$, é um homomorfismo. Se S for um subsemigrupo de $\mathbf{B}$ então $\nu(S)$ é um subsemigrupo de $\mathbb{Z}$. Se S é bilateral então $\nu(S)$ contém inteiros negativos e positivos simultaneamente, e portanto é um (sub)grupo. Por outras palavras, $\nu(S) = d\mathbb{Z}$, em que $d = \gcd(\lambda(S))$, e portanto existem $x, y \in \mathbf{B}$ com $\nu(x) = d$ e $\nu(y) = -d$. No que se segue construiremos dois de elementos "especiais", e depois usaremo-los para gerar todos os elementos de $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$. Para isso necessitamos resultado seguinte, da teoria de números:

Lema 3.11. *Sejam $a_1, \ldots, a_k, b_1, \ldots, b_l, r_0 \in \mathbb{N}_0$, arbitrários tais que $a_1 > 0$, $b_1 > 0$ e seja*

$$d = \gcd(a_1, \ldots, a_k, b_1, \ldots, b_l).$$

Então, existem números $\alpha_1, \ldots, \alpha_k, -\beta_1, \ldots, -\beta_l \in \mathbb{N}_0$ tais que:

(1) $\alpha_1 a_1 + \ldots + \alpha_k a_k + \beta_1 b_1 + \ldots + \beta_l b_l = d$;

(2) $\alpha_1, \ldots, \alpha_k, -\beta_1, \ldots, -\beta_l \geq r_0$.

Demonstração. Começamos por supor, sem perde de generalidade, que $a_1, \ldots, a_k$, $b_1, \ldots, b_l > 0$. Como $d = \gcd(a_1, \ldots, a_k, b_1, \ldots, b_l)$, podemos escrever $d = \sum_{i=1}^{k} \alpha'_i a_i + \sum_{j=1}^{l} \beta'_j b_j$ para alguns inteiros $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l$. Seja H um qualquer inteiro positivo e seja

$$P = Hkla_1 \ldots a_k b_1 \ldots b_l, \quad Q = P/k, \quad R = P/l.$$

Podemos então escrever

$$\begin{aligned} d &= \sum_{i=1}^{k} \alpha'_i a_i + \sum_{j=1}^{l} \beta'_j b_j = \sum_{i=1}^{k} \alpha'_i a_i + P - P + \sum_{j=1}^{l} \beta'_j b_j \\ &= \sum_{i=1}^{k} (\alpha'_i a_i + Q) + \sum_{j=1}^{l} (\beta'_j b_j - R) = \sum_{i=1}^{k} (\alpha'_i + Q/a_i) a_i + \sum_{j=1}^{l} (\beta'_j - R/b_j) b_j \\ &= \sum_{i=1}^{k} \alpha_i a_i + \sum_{j=1}^{l} \beta_j b_j \end{aligned}$$

é claro que um incremento um H reflecte-se num incremento também em $\alpha_1, \ldots, \alpha_k$, $-\beta_1, \ldots, -\beta_l$ e portanto o resultado mantém-se. □

Demonstração do Teorema 3.10. Seja $F_D = S \cap D \cap L_q$ e $S' = S \backslash F_D$. Temos $S' = S \cap (M_d \cap (S'_{q,p} \cup \Sigma_p))$ em que $d = \gcd(\lambda(S'))$ e portanto S' é um subsemigrupo. Note-se que os elementos $c^i b^i \in F_D$ actuam como identidades em S'. Seja $x \in S' \cap U$ e $y \in S' \cap \widehat{U}$ tais que $\Phi(x) = \iota(S) = q$ e $\Psi(y) = \kappa(S) = p$. Seja $Y \subseteq S'$ um conjunto finito de tal modo que:

(i) $x, y \in Y$;

(ii) $\Lambda_i \cap S' \cap S'_{q,p} \neq \emptyset \implies \Lambda_i \cap Y \neq \emptyset$ for $i \in \{q \ldots, p-1\}$ (Y contém pelo menos um representante por linha, na faixa com elementos em S');

(iii) $\{(i-p) \mod d : \Lambda_i \cap Y \cap \Sigma_p \neq \emptyset\} = \{(i-p) \mod d : \Lambda_i \cap S' \cap \Sigma_p \neq \emptyset\}$ (Y contém pelo menos um representante de cada classe de linhas, na grelha que contém um representante em S');

(iv) $\gcd(\lambda(Y)) = d$.

Tal Y pode ser obtido escolhendo um conjunto finito Y_1 (com, no máximo, $p-q+d$ elementos) que satisfaça de (i) a (iii), e um conjunto finito Y_2 tal que $\gcd(\lambda(Y_2)) = \gcd(\lambda(S'))$ e fazendo $Y = Y_1 \cup Y_2$. Seja $Y \cap (D \cup U) = \{c^{i_1} b^{j_1}, \ldots, c^{i_r} b^{j_r}\}$ em que $x = c^{i_1} b^{j_1}$, $q = i_1 \leq i_2 \leq \ldots \leq i_r, j_1 > i_1$, $j_2 \geq i_2, \ldots, j_r \geq i_r$ e seja $Y \cap \widehat{U} = \{c^{k_1} b^{l_1}, \ldots, c^{k_s} b^{l_s}\}$ com $y = c^{k_1} b^{l_1}$, $p = l_1 \leq l_2 \leq \ldots \leq l_s$ e $k_1 > l_1, \ldots, k_s > l_s$.

Mostraremos que

$$c^{p+d} b^p, \quad c^p b^{p+d} \in S'.$$

A observação seguinte, ilustrada na Figura 3.4, mostra a importância deste dois elementos.

Seja $c^i b^j$ um elemento de $M_d \cap (S_{q,p} \cup \Sigma_p)$. Sabemos que $c^i b^j c^p b^{p+d} = c^i b^{j+d}$ o que significa, intuitivamente, que podemos mover d posições para a direita usando

o elemento $c^p b^{p+d}$. Se $i \geq p$ então também temos que $c^{p+d}b^p c^i b^j = c^{i+d}c^j$ o que significa que podemos mover d posições para baixo. Se $j \geq p+d$ então $c^i b^j c^{p+d}c^p = c^i b^{j-d}$ o que significa que podemos mover para a direita. Finalmente, se $i \geq p+d$ então $c^p b^{p+d}c^i b^j = c^{i-d}b^j$ e portanto podemos mover-nos para cima.

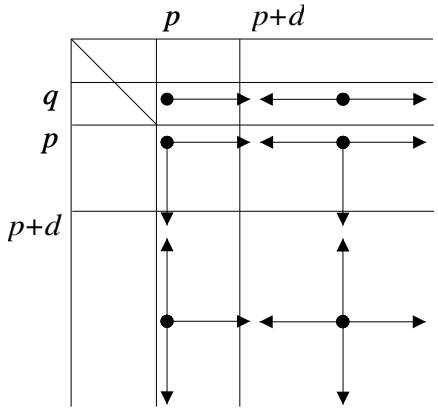


Figura 3.4: Movimento usando $c^p b^{p+d}$ e $c^{p+d}b^p$

Com o intuito de provar $c^{p+d}b^p, c^p b^{p+d} \in S'$ notemos que, por (iv), $d = \gcd\{j_1 - i_1, \ldots, j_r - i_r, k_1 - l_1, \ldots, k_s - l_s\}$. Uma vez que $i_1 - j_1 < 0$ e $k_1 - l_1 > 0$, aplicando o Lema 3.11 obtemos

$$d = \alpha_1(i_1 - j_1) + \ldots + \alpha_r(i_r - j_r) + \beta_1(k_1 - l_1) + \ldots + \beta_s(k_s - l_s) \tag{3.1}$$

com $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \geq \max\{i_1, \ldots, i_r, l_1, \ldots, l_s\}$. Consideremos agora o produto $(c^{i_1}b^{j_1})^{\alpha_1} \ldots (c^{i_r}b^{j_r})^{\alpha_r}$ que é igual a

$$(c^{i_1}b^{i_1+\alpha_1(j_1-i_1)})(c^{i_2}b^{i_2+\alpha_2(j_2-i_2)}) \ldots (c^{i_r}b^{i_r+\alpha_r(j_r-i_r)}).$$

Uma vez que $\alpha_1 \geq \max\{i_1, \ldots, i_r\}$ e $j_1 - i_1 \geq 1$, obtemos $i_1 + \alpha_1(j_1 - i_1) > i_1, \ldots, i_r$ e portanto, efectuando cálculos no produto anterior, a partir da esquerda, obtemos

$$c^{i_1}b^{i_1+\alpha_1(j_1-i_1)+\alpha_2(j_2-i_2)+\ldots+\alpha_r(j_r-i_r)}. \tag{3.2}$$

Consideremos agora o produto $(c^{k_s}b^{l_s})^{\beta_s} \ldots (c^{k_2}b^{l_2})^{\beta_2}(c^{k_1}b^{l_1})^{\beta_1}$ que é igual a

$$(c^{l_s+\beta_s(k_s-l_s)}b^{l_s}) \ldots (c^{l_2+\beta_2(k_2-l_2)}b^{l_2})(c^{l_1+\beta_1(k_1-l_1)}b^{l_1}).$$

Tendo em conta que $\beta_1 \geq \max\{l_1, \ldots, l_s\}$ e $k_1 - l_1 \geq 1$ temos que $l_1 + \beta_1(k_1 - l_1) > l_1, \ldots, l_s$, efectuando cálculos no produto anterior, a partir da direita, obtemos

$$c^{l_1+\beta_1(k_1-l_1)+\beta_2(k_2-l_2)+\ldots+\beta_s(k_s-l_s)}b^{l_1}. \tag{3.3}$$

Multiplicando o obtido em 3.2 e em 3.3 obtemos

$$c^{i_1}b^{i_1+\alpha_1(j_1-i_1)+\alpha_2(j_2-i_2)+\ldots+\alpha_r(j_r-i_r)}c^{l_1+\beta_1(k_1-l_1)+\beta_2(k_2-l_2)+\ldots+\beta_s(k_s-l_s)}b^{l_1}$$
$$= c^{l_1+d}b^{l_1} = c^{p+d}b^p$$

tendo em conta que $q = i_1 \leq l_1 = p$ e usando a Equação 3.1. Logo, $c^{p+d}b^p \in S'$. Como $d \mid (j_1 - i_1)$, podemos escrever $j_1 - i_1 = td$, para algum $t \in \mathbb{N}$. Uma vez que $p \geq i_1$ temos $p + td \geq j_1$ e portanto $c^{i_1}b^{j_1}(c^{p+d}b^p)^t = c^{i_1-j_1+p+td}b^p = c^pb^p$. Logo, concluímos também que $c^pb^p \in S'$. Consideremos agora as constantes $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \geq \max\{i_1, \ldots, i_r, l_1, \ldots, l_s\}$ de tal modo que

$$d = \alpha_1(j_1 - i_1) + \ldots + \alpha_r(j_r - i_r) + \beta_1(l_1 - k_1) + \ldots + \beta_s(l_s - k_s) \tag{3.4}$$

e consideremos também o seguinte elemento de S':

$$c^pb^pc^{i_1}b^{i_1+\alpha_1(j_1-i_1)+\alpha_2(j_2-i_2)+\ldots+\alpha_r(j_r-i_r)}c^{l_1+\beta_1(k_1-l_1)+\beta_2(k_2-l_2)+\ldots+\beta_s(k_s-l_s)}b^{l_1}.$$

Sabendo que $i_1 = q \leq p = l_1$, este elemento pode ser escrito como

$$c^pb^{p+\alpha_1(j_1-i_1)+\alpha_2(j_2-i_2)+\ldots+\alpha_r(j_r-i_r)}c^{p+\beta_1(k_1-l_1)+\beta_2(k_2-l_2)+\ldots+\beta_s(k_s-l_s)}b^p$$

e, pela Equação 3.4, isto é igual a c^pb^{p+d}. Portanto, temos que $c^pb^{p+d}, c^{p+d}b^p \in S'$, tal como pretendido.

Seguidamente provaremos que $S' \cap \Sigma_p = \Sigma_{p,d,P}$ em que $P = \{(i-p) \mod d : L_i \cap Y \cap \Sigma_p \neq \emptyset\}$. Comecemos por mostrar que

$$\Sigma_{p,d,P} \subseteq S'.$$

Consideremos $c^{p+r+ud}b^{p+r+vd} \in \Sigma_{p,d,P}$. Por definição de Y existe $c^ib^j \in Y \cap \Sigma_p$ de tal modo que $(i-p) \mod d = r$. Portanto, como $Y \subseteq S' \subseteq M_d$, obtemos $c^ib^j = c^{p+r+u'd}b^{p+r+v'd}$. Tal como já vimos, podemos mover-nos de c^ib^j para $c^{p+r+ud}b^{p+r+vd}$, usando os elementos c^pb^{p+d} e $c^{p+d}b^p$, o que significa que $c^{p+r+ud}b^{p+r+vd}$ pertence a S'.

Provemos agora que

$$S' \cap \Sigma_p \subseteq \Sigma_{p,d,P}.$$

Seja $c^ib^j \in S' \cap \Sigma_p$. Pela definição de P e por (iii), na definição de Y, temos $(i-p) \mod d = r \in P$. Como $S' \subseteq M_d$, temos $c^ib^j = c^{p+r+ud}b^{p+r+vd}$ para algum $u, v \geq 0$, logo, $c^ib^j \in \Sigma_{p,d,P}$. Assim concluímos que $S' \cap \Sigma_p = \Sigma_{p,d,P}$.

Demonstremos agora que $S' \cap S_{q,p} = \Lambda_{I,p,d}$, com $I = \{i : q \leq i \leq p-1; c^ib^j \in S' \text{ para algum } j\}$. De facto, para qualquer elemento $c^ib^j \in S' \cap S_{q,p}$ podemos mover-nos para a direita ou esquerda usando os elementos c^pb^{p+d} e $c^{p+d}b^p$ até obtermos

toda a linha $\Lambda_{i,p,d}$. Como $S' \subseteq M_d$ então $S' \cap S_{q,p} = \Lambda_{I,p,d}$. Concluímos então que $S' = F \cup \Sigma_{p,d,P} \cup \Lambda_{I,p,d}$ em que $F = S \cap T_{q,p}$ é um conjunto finito, e isto implica que $S = F_D \cup F \cup \Sigma_{p,d,P} \cup \Lambda_{I,p,d}$, tal como pretendido.

□

6 Subsemigrupos Superiores

Nesta secção vamos considerar subsemigrupos cujos elementos estão acima (ou na) diagonal. O caso em que todos os elementos estão abaixo (ou na) diagonal é obtido, tal como já foi dito, usando o anti-isomorfismo $\widehat{\ }$.

Lema 3.12. *Seja* $p, q, d \in \mathbb{N}_0$, *com* $q < p$, *e* $d > 0$, *e seja* $X \subseteq S'_{q,p}$ *um conjunto finito com* $\iota(X) = q$ *e* $\gcd(\lambda(X)) = d$. *Para qualquer* $x \in X$ *existe* $m \in \mathbb{N}_0$ *tal que*

$$\Lambda_{\Phi(x),m,d} \subseteq \langle X \rangle.$$

Demonstração. Sejam $S = \langle X \rangle$ e $Y = X \cap U = \{c^{i_1} b^{i_1+d_1}, \ldots, c^{i_n} b^{i_n+d_n}\}$ com $q = i_1 \leq i_2 \leq \ldots \leq i_n; d_1, \ldots, d_n \in \mathbb{N}$. Para cada $j \in \{1, \ldots, n\}$ escolhemos $\alpha_j \in \mathbb{N}$ de tal forma que $i_j + \alpha_j d_j \geq p$ e $d = \gcd(d_1, \ldots, d_n) = \gcd(\alpha_1 d_1, \ldots, \alpha_n d_n)$. Podemos considerar $\alpha_1, \ldots, \alpha_n$ como sendo números primos distintos suficientemente grandes de forma que não apareçam na decomposição de d em factores primos. É sabido que dados números $x_1, \ldots, x_n \in \mathbb{N}$, tais que $\gcd\{x_1, \ldots, x_n\} = d$, existe uma constante k tal que todos os múltiplos de d maiores que k podem ser obtidos como combinações de $x_1, \ldots, x_n$, com coeficientes em $\mathbb{N}$. Seja $k \in \mathbb{N}$ de tal modo que

$$\{td : td \geq k, t \in \mathbb{N}\} \subseteq \{\gamma_1(\alpha_1 d_1) + \ldots + \gamma_n(\alpha_n d_n) : \gamma_1, \ldots, \gamma_n \in \mathbb{N}\}.$$

Seja $m = p + k$. Vamos provar que $\Lambda_{\Phi(x),m,d} \subseteq S$ para qualquer $x \in X$. Seja $i = \Phi(x) \in \{q, \ldots, p-1\}$ e $t \in \mathbb{N}$ com $i + td \geq m$. Então $td \geq m - i = p + k - i \geq k$. Portanto, podemos escrever

$$td = \gamma_1(\alpha_1 d_1) + \ldots + \gamma_n(\alpha_n d_n)$$

com $\gamma_1, \ldots, \gamma_n \in \mathbb{N}$. Se $x = c^{i_j} c^{i_j+d_j} \in Y$ então temos

$$c^i b^{i+td} = c^{i_j} b^{i_j+td} = (c^{i_j} b^{i_j+\alpha_j d_j})^{\gamma_j} \cdot \prod_{\substack{1 \leq l \leq n \\ l \neq j}} (c^{i_l} b^{i_l+\alpha_l d_l})^{\gamma_l}.$$

Se $x \notin Y$ então $x = c^i b^i$ e assim temos $c^i b^{i+td} = c^i b^i (c^{i_1} b^{i_1+\alpha_1 d_1})^{\gamma_1} \dots (c^{i_n} b^{i_n+\alpha_n d_n})^{\gamma_n} \in S$, tal como pretendíamos demonstrar. □

Teorema 3.13. *Seja S é um subsemigrupo de $\boldsymbol{B}$ tal que $S \cap \widehat{U} = \emptyset$ e $S \cap U \neq \emptyset$. Existe $d \in \mathbb{N}$, $I \subseteq \mathbb{N}_0$, $F_D \subseteq D \cap L_{\min(I)}$, e conjuntos $S_i \subseteq \Lambda_{i,i,d}$ $(i \in I)$ tais que*

$$S = F_D \cup \bigcup_{i \in I} S_i$$

em que cada S_i tem a forma

$$S_i = F_i \cup \Lambda_{i,m_i,d}$$

para algum $m_i \in \mathbb{N}_0$, algum conjunto finito F_i, e

$$I = I_0 \cup \{r + ud : r \in R, u \in \mathbb{N}_0, r + ud \geq N\}$$

para algum (possivelmente vazio) $R \subseteq \{0, \dots, d-1\}$, algum $N \in \mathbb{N}_0$ e algum conjunto finito $I_0 \subseteq \{0, \dots, N-1\}$.

Demonstração. Seja $q = \iota(S)$, $F_D = S \cap D \cap L_q$, $S' = S \backslash F_D$, temos então $S = F_D \cup S'$, e seja $d = \gcd(\lambda(S'))$. Uma vez que $S' \subseteq (U \cup D) \cap M_d$, fazendo $I = \Phi(S')$, temos $S = F_D \cup \bigcup_{i \in I} S_i$ em que $S_i = S' \cap \Lambda_{i,i,d}$ para $i \in I$. Para qualquer $i \in I$ podemos considerar o conjunto finito $X_i \subseteq S'$ com $i \in \Phi(X_i)$ e $\gcd(X_i) = d$ e concluímos, usando o Lema 3.12, que $\Lambda_{i,m_i,d} \subseteq S$ para algum $m_i \in \mathbb{N}_0$. Se I for finito então, podemos considerar $R = \emptyset$, $I_0 = I$ e $N = \max(I) + 1$. Agora vamos considerar o caso em que I é infinito. Seja $X = \{c^{i_1} b^{i_1+d_1}, \dots, c^{i_k} b^{i_k+d_k}\} \subseteq S'$ tal que $d = \gcd(\lambda(X))$, $i_1 \geq i_2 \geq \dots \geq i_k$. Pelo Lema 3.12, existe uma constante M tal que $td \geq M$ implica $c^{i_1} b^{i_1+td} \in S'$. Definir um conjunto $R \subseteq \{0, \dots, d-1\}$ como sendo

$$r \in R \Leftrightarrow |\{i \in \mathbb{N} : \Lambda_i \cap S' \neq \emptyset \ \&\ i \bmod d = r\}| = \infty.$$

□

Então existe uma constante K tal que

$$c^i b^j \in S' \ \&\ i \geq K \implies (i \bmod d) \in R.$$

seja $N = \max\{i_1, K\}$ e

$$I_0 = \{i : q \leq i \leq N-1, \Lambda_i \cap S' \neq \emptyset\}.$$

Achamos que

$$I = I_0 \cup \{r + ud : r \in R, u \in \mathbb{N}_0, r + ud \geq N\}.$$

A inclusão directa é obvia, tal como $I_0 \subseteq I$. Consideremos agora um arbitrário $r + ud \geq N$, $r \in R$. Seja um arbitrário $c^{r+vd}b^{r+vd+wd} \in S'$ tal que $t = v - u \geq M/d$. De $td \geq M$ sai que $c^{i_1}b^{i_1+td} \in S'$ e portanto $c^{i_1}b^{i_1+td}c^{r+vd}b^{r+vd+wd} = c^{r+ud}b^{r+vd+wd} \in S'$ porque $r + vd = r + ud + td \geq N + td \geq i_1 + td$. Concluímos então que $r + ud \in I$.

Observação 3.14. No caso em que I é finito ($R = \emptyset$), o subsemigrupo pode ser escrito como a reunião de dois subconjuntos finitos e muitas linhas finitas todas começadas na mesma coluna. Formalmente, existem $q, p, m \in \mathbb{N}_0$ com $q < p \leq m$, conjuntos finitos $F_D \subseteq D \cap L_q$, $F \subseteq S'_{q,p} \backslash S_{q,p,m}$ e um conjunto finito $I \subseteq \{q, \ldots, p-1\}$ tal que

$$S = F_D \cup F \cup \Lambda_{I,m,d}.$$

7 Corolários

Nesta secção usaremos a nossa classificação de subsemigrupos de $\mathbf{B}$ para descrever qual deles é regular (e portanto inverso), simples ou bisimples. Em particular, é sabido que em $\mathbf{B}$ temos

$$c^ib^j \mathcal{L}\, c^kb^l \Leftrightarrow j = l, \quad c^ib^j \mathcal{R}\, c^kb^l \Leftrightarrow i = k, \quad c^ib^j \mathcal{H}\, c^kb^l \Leftrightarrow i = k \,\&\, j = l,$$

$$\mathcal{D} = \mathcal{J} = \mathbf{B} \times \mathbf{B}.$$

Nós vimos que $\mathbf{B}$ é um semigrupo bisimples (i.e. tem uma única $\mathcal{D} - classe$, a "egg-box"que é familiar da grelha quadrada apresentada anteriormente). Uma vez que os idempotentes são os elementos da diagonal, um elemento c^ib^j tem um único inverso c^jb^i, e $\mathbf{B}$ é um semigrupo inverso. Logo, um subsemigrupo S de $\mathbf{B}$ é regular se e só se for inverso se e só se satisfaz $c^ib^j \in S \implies c^jb^i \in S$. Temos portanto:

Teorema 3.15. *Um subsemigrupo S de $\mathbf{B}$ é regular (e portanto inverso) se e só se tiver a forma $F_D \cup \Sigma_{p,d,P}$ em que F_D é um subconjunto finito da diagonal e quer F_D quer P podem ser vazios.*

De facto, $\mathbf{B}$ é um ω-semigrupo inverso, o que significa que os seus semireticulados de idempotentes são isomorfos aos números naturais ordenados por $\geq$. É obvio que, cada subsemigrupo inverso S de $\mathbf{B}$ terá a mesma propriedade. Logo, por [28], S é

uma extensão do seu ideal minimal bilateral K por uma cadeia finita da grupos C. Sendo ω-semigrupo inverso simples, K é isomorfo a uma extensão de Bruck-Reilly de uma cadeia finita da grupos; ver detalhes em [23], [28] ou [18, Sec. 5.7]. Uma vez que, na adição, as $\mathcal{H}$-classes de K são triviais, sai que todos os grupos são triviais, e obtemos que K é isomorfo a M_d (B_d na notação original do Munn). No contexto do Teorema 3.15 temos $C = F_D$ e $K = \Sigma_{p,d,P}$.

Do Teorema 3.15, ou da discussão anterior, observando que um subsemigrupo da forma $\Sigma_{p,d,r}$ é isomorfo a $\mathbf{B}$, obtemos:

Corolário 3.16. *Uma $\mathcal{D}$-classe de um subsemigrupo regular $\boldsymbol{B}$ ou é isomorfo a $\boldsymbol{B}$ ou é um grupo trivial.*

O resultado seguinte é necessário para determinar os subsemigrupos simples de $\mathbf{B}$:

Lema 3.17. *Um subconjunto da forma $I_p = \{c^i b^j : 0 \leq i \leq j, j \geq p\}$ ($p \in \mathbb{N}_0$) é um ideal de U.*

A demonstração deste lema encontra-se em [27].

Teorema 3.18. *Os subsemigrupos simples de $\boldsymbol{B}$ são precisamente aqueles da forma $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ e $\widehat{\Lambda_{I,p,d}} \cup \Sigma_{p,d,P}$ (com P um conjunto diferente do vazio).*

Demonstração. Um subsemigrupo superior (ou diagonal) S não é simples uma vez que, para p suficientemente grande o conjunto $S \cap I_p$ é um ideal próprio de S; de modo análogo, um subsemigrupo inferior não é simples. Um subsemigrupo bilateral S da forma $F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ não é simples se $F_D \cup F \neq \emptyset$, porque neste caso $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ é um ideal próprio de S. Isto prova que um subsemigrupo simples de $\mathbf{B}$ deve ser da forma $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ ou $\widehat{\Lambda_{I,p,d}} \cup \Sigma_{p,d,P}$. Para o reciproco, provaremos agora que um subsemigrupo S da forma $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ é sempre simples, mostrando que, para um $s = c^k b^l \in S$ arbitrário, temos $S \subseteq S^1 s S^1$. Seja $t = c^i b^j \in S$ arbitrário. Fazendo $\alpha = c^i b^u \in S$ com $u \geq \max(k, j + k - l)$ temos $\alpha s = c^i b^{u-k+l}$. Assim, com $\beta = c^{p+d} b^p \in S$ e $v = (u - k + l - j)/d$, obtemos $\alpha s \beta^v = c^i b^{u-k+l} c^{p+vd} b^p = t$. □

Teorema 3.19. *Um subsemigrupo de $\boldsymbol{B}$ é bisimples se e só se tiver a forma $\Sigma_{p,d,0}$.*

Demonstração. Seja S um subsemigrupo simples arbitrário de $\mathbf{B}$. Sem perda de generalidade podemos assumir que S é da forma $S = \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ com $0 \in P$.

Se S contiver dois elementos $\alpha = c^i b^j$, $\beta = c^k b^l$ tal que $i - p \mod d \neq k - p \mod d$ então S não é bisimples. De facto, supondo que α e β estão $\mathcal{D}$-relacionados em S, então existe $s \in S$ tal que $\alpha \mathcal{R}^S s$ e $s \mathcal{R}^S \beta$. Isto implica que $\alpha \mathcal{L}^{\mathbf{B}} s$ e $s \mathcal{R}^{\mathbf{B}} \beta$ logo, $s = c^k b^j$. Mas d não divide $k - j$ logo $s \notin S$, o que é uma contradição. Portanto, para S ser bisimples é necessário que $P = \{0\}$ e, pelo Lema 3.9, que $I = \{p - ud : p - ud \geq k\}$ para algum $k \geq 0$. Note-se agora que, os elementos $c^p b^p$ e $c^{p-d} b^p$ não estão $\mathcal{L}$-relacionados em S porque, para um qualquer $c^k b^l \in S$ temos $l \geq p$ e assim, $c^k b^l c^{p-d} b^p = c^k b^{l+d} \neq c^p b^p$. Suponhamos que $c^p b^p \mathcal{D}^S c^{p-d} b^p$, então, teremos $c^p b^p \mathcal{L}^S s$ e $s \mathcal{R}^S c^{p-d} b^p$ para algum $s \in S$ e portanto, $c^p b^p \mathcal{L}^{\mathbf{B}} s$ e $s \mathcal{R}^{\mathbf{B}} c^{p-d} b^p$ o que implica $s = c^{p-d} b^p$, logo, $c^p b^p \mathcal{L}^S c^{p-d} b^p$, o que é uma contradição. Logo, para que S seja bisimples é de facto necessário que $I = \emptyset$ e $P = \{0\}$. Como $\Sigma_{p,d,0}$ é isomorfo a $\mathbf{B}$ é bisimples, o que completa a demonstração. □

Seguidamente descreveremos subsemigrupos bilaterais como uma reunião finita de semigrupos.

Teorema 3.20. *Um subsemigrupo bilateral é uma reunião finita de cópias de $\boldsymbol{B}$ e subsemigrupos de $\mathbb{N}_0$.*

Demonstração. Suponhamos, sem perda de generalidade, que S é da forma $S = F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$. Temos $S = \bigcup_{i=0}^{p-1} (S \cap \Lambda_{i,i,d}) \cup \bigcup_{r \in P} \Sigma_{p,d,r}$ com $\Lambda_{i,i,d}$ isomorfo a $\mathbb{N}_0$ através de $c^i b^{i+ud} \mapsto u$ e $\Sigma_{p,d,r}$ isomorfo a $\mathbf{B}$, donde sai o pretendido. □

Dizemos que M é um subsemigrupo *especial* de $\mathbb{N}_0$ se $M = \{n : n \geq k\}$ para algum k.

Corolário 3.21. *Um subsemigrupo de $\boldsymbol{B}$ é:*

(1) *É regular se e só se se puder obter adicionando sucessivamente um número finito de identidades a uma reunião finita de cópias de $\boldsymbol{B}$;*

(2) *simples se e só se é reunião finita de cópias de $\boldsymbol{B}$ e subsemigrupos especiais de $\mathbb{N}_0$;*

(3) *bisimples se e só se é isomorfo a $\boldsymbol{B}$.*

8 Cálculo de Parâmetros e Exemplos

Nesta secção mostraremos como determinar os parâmetros que aparecem no nosso teorema principal, dado um conjunto finito gerador para o subsemigrupo. Começamos por considerar os subsemigrupos bilaterais definidos pela condição (2)(i) no teorema principal e depois consideremos subsemigrupos superiores finitamente gerados, definidos pela condição (3)(i), observando novamente que os subsemigrupos definidos em (2)(ii) e (3)(ii) se podem obter destes dois usando o anti-isomorfismo $\widehat{\ }$. Observamos que, dado um conjunto finito X, conseguimos determinar que tipo de subsemigrupos ele gera:

(1) $\langle X\rangle \subseteq D$ se e só se $X \subseteq D$;

(2) $\langle X\rangle$ é um subsemigrupo bilateral se e só se $X \cap U \neq \emptyset$ e $X \cap \widehat{U} \neq \emptyset$;

(3) $\langle X\rangle$ é um subsemigrupo superior (respectivamente inferior) se e só se $X \cap U \neq \emptyset$ e $X \cap \widehat{U} = \emptyset$ (respectivamente $X \cap U = \emptyset$ e $X \cap \widehat{U} \neq \emptyset$).

Teorema 3.22. *Seja $S = F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ um subsemigrupo bilateral de $\boldsymbol{B}$ definido pela condição (2)(i) no teorema principal. Seja X um conjunto gerador de S. Então temos:*

(1) $q = \iota(X)$, $p = \kappa(X)$, $d = \gcd(\lambda(X))$;

(2) $F_D = X \cap D \cap L_q$;

(3) $P = \{(i-p) \mod d : \Lambda_i \cap X \cap \Sigma_p \neq \emptyset\}$;

(4) $F = \bigcup_{i=1}^{M} (X \cap T_{q,p})^i \cap T_{q,p}$ *em que* $M = (p-q+1)(p-q)/2$;

(5) *Definindo*

$$I_0 = \{p+r-ud : r \in P,\ u \in \mathbb{N}_0,\ p+r-ud \geq q\} \cup \{i : \Lambda_i \cap (F \cup (X \cap S_{q,p})) \neq \emptyset\}$$

e a acção esquerda $. : \mathbf{B} \times \mathbb{N}_0 \to \mathbb{N}_0$ *por*

$$c^i b^j . k = \begin{cases} i & \text{caso } j \geq k \\ i-j+k & \text{caso contrário} \end{cases}$$

obtemos

$$I = \bigcup_{n=0}^{p-q} F^n . I_0.$$

DEMONSTRAÇÃO. Seja $q' = \iota(X)$, $p' = \kappa(X)$, $d' = \gcd(\lambda(X))$, $F'_D = X \cap D \cap L_{q'}$ e $X' = X \backslash F'_D$. Então temos $S = F'_D \cup \langle X' \rangle$ e os elementos de F'_D actuam como identidades em $\langle X' \rangle$. Caso $q' \leq p'$ então $X' \subseteq M_d \cap (S'_{q',p'} \cup \Sigma_{p'})$ e, pelos Lemas 3.2 e 3.4, este último conjunto é um subsemigrupo e consequentemente, $\langle X' \rangle \subseteq M_d \cap (S'_{q',p'} \cup \Sigma_{p'})$, implicando $q = q'$, $p = p'$. Caso $q' > p'$ então, por raciocínio análogo temos $\langle X' \rangle \subseteq M_d \cap (\widehat{S'_{q',p'}} \cup \Sigma_{p'})$ donde sai que $p = q' < p' = q$ o que contradiz a nossa suposição sobre a forma de S. Portanto, temos $q = q'$, $p = p'$ sai imediatamente que $F_D = F'_D = X \cap D \cap L_{q'} = X \cap D \cap L_q$. E por fim, de $S = \langle X \rangle \subseteq M_{d'}$ (uma vez que $M_{d'}$ é um semigrupo) sai que $d = d'$. Isto prova (1) e (2).

Sabemos que $P = \{(i-p) \mod d : \Lambda_i \cap S \cap \Sigma_p \neq \emptyset\}$. Seja $P' = \{(i-p) \mod d : \Lambda_i \cap X' \cap \Sigma_p \neq \emptyset\}$. É claro que $P' \subseteq P$. Também temos $X' \subseteq \Sigma_{p,d,P} \cup (M_d \cap S'_{q,p}) = T$. Mas T, pelo Lema 3.7, é um subsemigrupo, e assim $\langle X' \rangle = S \backslash F_D \subseteq T$. Portanto $S \cap \Sigma_p \subseteq T \cap \Sigma_p$, o que é equivalente a $\Sigma_{p,d,P} \subseteq \Sigma_{p,d,P'}$, logo, $P = P'$, o que prova (3).

Para provar (4) observe-se que as inclusões no Lema 3.5 implicam que $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ seja um ideal de S. Consequentemente sai que os elementos de F se podem obter formando um produto adequado de geradores de X que pertencem a $T_{q,p}$. Como $T_{q,p}$ tem $(p-q+1)(p-q)/2$ elementos sai a formula desejada. Na prática não necessitamos de formar todos estes produtos. Usando novamente o facto de que $\Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ é um ideal vimos que F pode ser determinado pelo seguinte algoritmo:

$X_0 := X \cap T_{q,p}$
$F := X_0$
while not $(FX_0 \cap T_{q,p} \subseteq F)$ do
  $F := F \cup (FX_0 \cap T_{q,p})$
od.

Para provar (5) mostraremos primeiro que $I_0 \subseteq I$. Tendo em conta que $S \cap (S_{q,p} \cup \Sigma_p) = \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$ é um subsemigrupo, do Lema 3.9 tiramos que $\{p + r - ud : r \in P, u \in \mathbb{N}_0, p + r - ud \geq q\} \subseteq I$. Dado $c^i b^j \in F \cup (X \cap S_{q,p})$, para obtermos um elemento em $S \cap (\Lambda_i \cup S_{q,p})$, podemos multiplicar este elemento à direita por uma potência de um elemento da forma $c^q b^{q+d_1}$ com $d_1 > 0$ (tal elemento existe pela definição de q). Deste elemento podemos obter a linha completa $\Lambda_{i,p,d}$ usando os elementos $c^p b^{p+d}, c^{p+d} b^p \in T$ e assim $I_0 \subseteq I$.

Seguidamente mostraremos que $T = \Lambda_{I_0,p,d} \cup \Sigma_{p,d,P}$ é um ideal direito ($TS^1 \subseteq T$). Sabemos que T é um subsemigrupo, pelo Lema 3.9. Pela forma como definimos I_0

obtemos $X \cap S_{q,p} \subseteq T$. Temos também que $X \cap \Sigma_p \subseteq T$ porque $S \cap \Sigma_p = \Sigma_{p,d,P} = T \cap \Sigma_p$. Falta-nos mostrar que $T((X \cap T_{q,p}) \cup F_D) \subseteq T$. Seja $c^k b^l \in T$, $c^i b^{i+d_1} \in (X \cap T_{q,p}) \cup F_D$. Tendo em conta que $l \geq i$, obtemos $c^k b^l c^i b^{i+d_1} = c^k b^{l+d_1} \in T$. Portanto T é um ideal direito. É obvio que $I_0 \subseteq I' \subseteq I$ logo $T' = \Lambda_{I',p,d} \cup \Sigma_{p,d,P}$ é também um ideal direito.

Note-se por fim que, embora se obtenha um elemento numa linha pertencente a $I \backslash I_0$, multiplicando dois elementos de F, não temos que considerar estes produtos com o fim de obter I. Se $c^i b^j$, $c^k b^l \in F$ e $c^i b^j c^k b^l = c^{i-j+k} b^l$ em que $i-j+k \in I \backslash I_0$, então I_0 contém a linha k e assim a linha $i-j+k$ pode também ser obtida através de $F \cdot I_0$. Concluímos que I, começando por I_0, se pode obter fazendo correr o algoritmo:

$I := I_0$
while not $(F.I \subseteq I)$ do
  $I := I \cup F.I$
od.

Este algoritmo não deve fazer mais do que $p-q$ iterações porque gera uma cadeia estritamente ascendente de conjuntos contidos em $\{q, \ldots, p-1\}$ (normalmente são necessárias muito menos iterações) o que conclui a prova de (5). □

Consideremos agora subsemigrupos superiores finitamente gerados. Seja $X \subseteq U \cup D$ um conjunto finito tal que $X \cap U \neq \emptyset$ e seja $S = \langle X \rangle$. Tal como na Observação 3.14, estamos no caso em que I é finito ($R = \emptyset$) na condição (3)(i) do teorema principal, e o nosso subsemigrupo assume a forma

$$S = F_D \cup F \cup \Lambda_{I,m,d}.$$

Tal como na demonstração do Teorema 3.22 podemos ver que

$$q = \iota(X), \quad p = \max(\Phi(X)) + 1, \quad I \subseteq \{q, \ldots, p-1\},$$

$$F_D = X \cap D \cap L_q, \quad d = \gcd(\lambda(X)).$$

Necessitamos de obter os parâmetros F, I e m do conjunto gerador. Como os elementos de F_D funcionam como identidades de $\langle X' \rangle$, em que $X' = X \backslash F_D$, assumiremos, sem perda de generalidade, que $F_D = \emptyset$, logo, $X = X' \subseteq S'_{q,p}$. Definiremos um algoritmo para obter estes parâmetros que consiste em formar uma sequência de reuniões de potências do conjunto gerador, X, $X \cup X^2$, $X \cup X^2 \cup X^3, \ldots$, até termos um subsemigrupo da forma $F \cup \Lambda_{I,m,d}$. Para isso necessitamos de uma

condição suficiente, que possa ser verificada por algoritmo, para um subconjunto finito de uma faixa que nos dê um subsemigrupo desta forma.

Lema 3.23. *Seja* $Y \subseteq S'_{q,p}$ *um conjunto finito com* $\gcd(Y) = d$ *e* $c^q b^{q+d_1} \in Y$ *para algum* $d_1 \in \mathbb{N}$. *Suponhamos que para qualquer* $i \in I = \Phi(Y)$ *existe* $m_i \in \mathbb{N}_0$ *tal que*

$$c^i b^{m_i}, b^{m_i+d}, \ldots, c^i b^{2m_i-i-d} \in Y,\ c^i b^{m_i-d} \notin Y.$$

Seja $m = \max\{m_i : i \in I\}$ *e* $F = Y \cap (S'_{q,p} \backslash S_{q,p,m})$. *Se* $FF \cap (S'_{q,p} \backslash S_{q,p,m}) \subseteq F$ *e* $F \cdot I \subseteq I$ *então* $\langle Y \rangle = F \cup \Lambda_{I,m,d}$. *Além disso,* m *é um mínimo de tal modo* $\Lambda_{I,m,d} \subseteq \langle Y \rangle$.

Demonstração. Começamos por mostrar que $F \cup \Lambda_{I,m,d} \subseteq \langle Y \rangle = S$. Para qualquer $i \in I$, temos $\Lambda_{i,m_i,d} \subseteq \langle c^i b^{m_i}, \ldots, c^i b^{2m_i-i-d} \rangle$, porque qualquer elemento de $\Lambda_{i,m_i,d}$ se pode escrever na forma $c^i b^u (c^i b^{m_i})^k$ para algum $k \in \mathbb{N}_0$, e $u \in \mathbb{N}_0$ tal que $i + (m_i - i) = m_i \leq u \leq 2m_i - i - d = i + 2(m_i - i) - d$. Concluímos que $\Lambda_{i,m_i,d} \subseteq S$ para algum $i \in I$ e portanto $F \cup \Lambda_{I,m,d} \subseteq S$ com $m = \max\{m_i : i \in I\}$. É claro que $Y \subseteq F \cup \Lambda_{I,m,d}$, porque $Y \subseteq M_d$ e $I = \Phi(Y)$, então, para provar a outra inclusão basta-nos mostrar que $F \cup \Lambda_{I,m,d}$ é um subsemigrupo. Temos que $FF \cap (S'_{q,p} \backslash S_{q,p,m}) \subseteq F$, $F \cdot I \subseteq I$ por hipótese e, como $\Phi(F) \subseteq I$, também temos que $\Phi(FF) \subseteq F \cdot I \subseteq I$ e concluímos que $FF \subseteq F \cup \Lambda_{I,m,d}$. É também claro $\Lambda_{I,m,d}(\Lambda_{I,m,d} \cup F) \subseteq \Lambda_{I,m,d}$. E por fim, $F \cdot I \subseteq I$ implica $F\Lambda_{I,m,d} \subseteq \Lambda_{I,m,d}$.

□

É claro que pode ser testado por um algoritmo se um conjunto finito $Y \subseteq S'_{q,p}$ satisfaz as condições do Lema 3.23; chamaremos a tal algoritmo *iscomplete (Y)* . Também precavendo que Y satisfaça estas condições, existe um algoritmo, *parâmetros(Y)*, que nos devolve o terno (F, I, m). Dados estes dois algoritmos, um algoritmo para determinar os parâmetros F, I, m, dado qualquer conjunto finito gerador X, é:

$Y := X$
while not $iscomplete(Y)$ do
  $Y := Y \cup YX$
od
$(F, I, m) := parameters(Y)$.

Note-se que, se estamos simplesmente interessados no conjunto de indices I de linhas em S, um algoritmo seguinte é muito mais eficiente:

$I := \Phi(X)$
while not $X \cdot I \subseteq I$ do
  $I := I \cup X \cdot I$
od.

Seguidamente apresentamos um exemplo de um subsemigrupo bilateral e outro de um subsemigrupo superior.

Exemplo 3.24. *Seja S um subsemigrupo de $\boldsymbol{B}$ gerado pelo*

$$X = \{cb, c^4b^7, c^{10}b^{13}, c^{18}b^{24}, c^{23}b^{17}\}.$$

É claro que S é um subsemigrupo bilateral da forma $S = F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}$. Do conjunto gerador vemos que $F_D = \{cb\}$, $q = 4$, $p = 17$, $d = 3$ e $P = \{0, 1\}$. Os restantes parâmetros obtém-se usando a nossa implementação dos algoritmos anteriores no sistema GAP (ver [9]), e eles são

$$I = \{4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15\}$$

e

$$F = \{c^4b^7, c^4b^{10}, c^4b^{13}, c^4b^{16}, c^7b^{13}, c^7b^{16}, c^{10}b^{13}, c^{10}b^{16}\}.$$

Podemos ver este subsemigrupo na figura 3.5.

Exemplo 3.25. *Seja S um subsemigrupo de B gerado pelo conjunto*

$$X = \{cb, c^3b^{13}, c^5b^9, c^{10}b^{16}\}.$$

É claro que S é um subsemigrupo superior da forma $S = F_D \cup F \cup \Lambda_{I,m,d}$ e do conjunto gerador vimos que $F_D = \{cb\}$ e $d = 2$. Usando novamente a implementação em GAP obtemos $m = 20$, $I = \{3, 5, 6, 10\}$ e

$$F = \{c^3b^{13}, c^3b^{17}, c^3b^{19}, c^5b^9, c^5b^{13}, c^5b^{17}, c^5b^{19}, c^6b^{16}, c^{10}b^{16}\}.$$

Podemos ver este subsemigrupo na figura 3.6.

9 Propriedades dos Subsemigrupos do Monoide Bicíclico

O monoide bicíclico é um dos semigrupos mais importante, com propriedades e generalizações notáveis; ver [1, 4, 11, 17, 18, 26, 27, 34, 35]

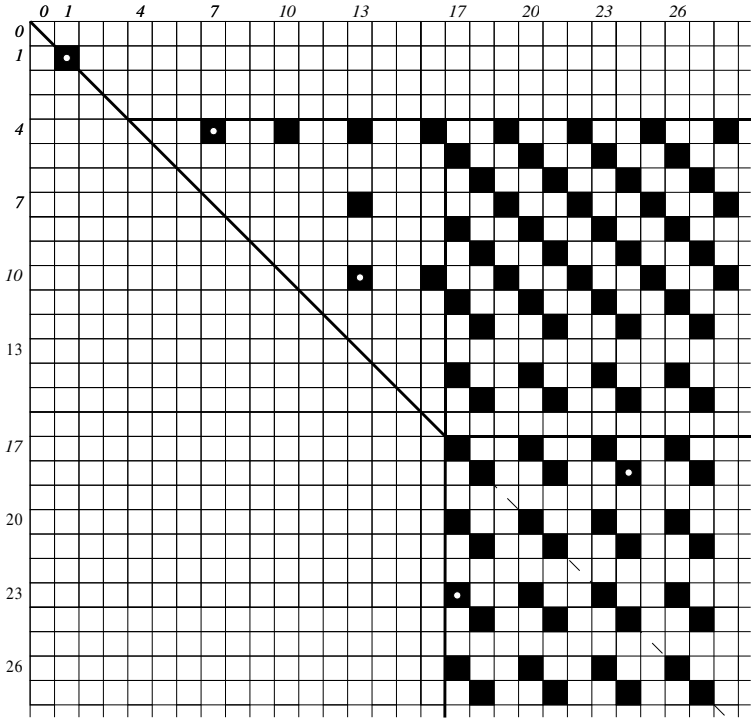


Figura 3.5: Subsemigrupo bilateral gerado por $\{cb, c^4b^7, c^{10}b^{13}, c^{18}b^{24}, c^{23}b^{17}\}$.

Nesta secção usaremos a descrição de subsemigrupos do monoide bicíclico, feitas nas secções anteriores, para estabelecer algumas das suas propriedades. Começaremos por mostrar que todos os subsemigrupos finitamente gerados são automáticos e finitamente apresentados. E por fim provaremos que um subsemigrupo de $\mathbf{B}$ é residualmente finito se e só se não contiver uma cópia de $\mathbf{B}$.

9.1 Geração Finita

Se A for um conjunto finito, denotemos por A^+ o subsemigrupo livre gerado por A, formado por palavras não vazias de A sob a concatenação, e por A^* o monoide livre gerado por A que consiste em A^+ com a palavra vazia ϵ. Seja S um semigrupo e $\psi : A \to S$ uma aplicação. Dizemos que A é um *conjunto gerador de S com respeito a ψ* se a única extensão de ψ a um semigrupo homomorfismo $\psi : A^+ \to S$ é sobrejectiva. Para $u, v \in A^+$ escrevemos $u \equiv v$ quando u e v são iguais como palavras e $u = v$ quando u e v representam o mesmo elemento no semigrupo i.e. $u\psi = v\psi$.

Nesta subsecção estabeleceremos condições necessárias e suficientes para que um subsemigrupo de um monoide bicíclico seja finitamente gerado provando o seguinte:

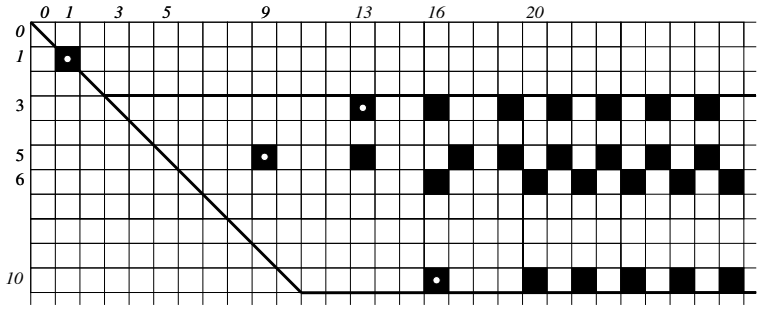


Figura 3.6: Subsemigrupo superior gerado por $\{cb, c^3b^{13}, c^5b^9, c^{10}b^{16}\}$.

Teorema 3.26. *Seja S um subsemigrupo de um monoide bicíclico. Então S é finitamente gerado se e só se verificar uma das seguintes condições:*

(i) S é um subsemigrupo diagonal finito;

(ii) S é um subsemigrupo bilateral;

(iii) S é um subsemigrupo superior e o conjunto $\{i \in \mathbb{N}_0 : L_i \cap S \neq \emptyset\}$ é finito;

(iv) S é um subsemigrupo inferior e o conjunto $\{i \in \mathbb{N}_0 : \widehat{L}_i \cap S \neq \emptyset\}$ é finito.

Demonstração. (i) Um subsemigrupo de um monoide bicíclico contido na diagonal apenas se admite a ele próprio como conjunto gerador e portanto é finitamente gerado se e só se for finito.

(ii) Seja $\iota(S) = q$, $\kappa(S) = p$ e $d = \gcd(\lambda(X))$. Podemos considerar, sem perda de generalidade, que $q \leq p$. Pelo Teorema 3.1 temos

$$S = F_D \cup F \cup \Sigma_{p,d,P} \cup \Lambda_{I,p,d}$$

em que F e F_D são conjuntos finitos e $I \subseteq \{q, q+1, \ldots, p-1\}$ para algum $q, p \in \mathbb{N}_0$. Seja, para cada $i \in I$, $i + u_i d = \min\{i + ud : i + ud \geq p\}$. Provaremos que o conjunto finito

$$Y = \{c^i b^{i+u_i d} : i \in I\} \cup \{c^p b^{p+d}, c^{p+d} b^p\} \cup \{c^{p+r} b^{p+r} : r \in P\}$$

gera o subsemigrupo $\Sigma_{p,d,P} \cup \Lambda_{I,p,d}$. Na verdade, para $c^i b^{i+ud} \in \Lambda_{I,p,d}$ temos $c^i b^{i+ud} = c^i b^{i+u_i d}(c^p b^{p+d})^{u-u_i}$, enquanto que para $c^{p+r+ud} b^{p+r+vd} \in \Sigma_{p,d,P}$ temos

$$c^{p+r+ud} b^{p+r+vd} = (c^{p+d} b^p)^u (c^{p+r} b^{p+r})(c^p b^{p+d})^v.$$

Portanto, todo o S pode ser gerado pelo conjunto finito $F_D \cup F \cup Y$. Em alternativa, podemos ver S como uma reunião finita de subsemigrupo de $\mathbb{N}$ e cópias de $\mathbf{B}$, tal como já vimos nas secções anteriores.

(*iii*) Provaremos que um subsemigrupo superior S é finitamente gerado se e só se o conjunto

$$K = \{i \in \mathbb{N}_0 : L_i \cap S \neq \emptyset\}$$

for finito. Primeiro, supomos que K é infinito e provamos que S não é finitamente gerado. Suponhamos que existe um conjunto finito X tal que $S = \langle X \rangle$. Como $X \subseteq S \subseteq U \cup D$ e X é finito, então $X \subseteq S'_{0,p}$ para algum $p \in \mathbb{N}_0$. Assim, $S = \langle X \rangle \subseteq S'_{0,p}$ porque, pelo Teorema 3.1, $S'_{0,p}$ é um subsemigrupo, e portanto $K \subseteq \{0, \ldots, p\}$ é finito, o que contradiz suposição. Concluímos então que S não é finitamente gerado.

Suponhamos agora que K é finito, então para provar que S é finitamente gerado basta observar que S é uma reunião finita de subsemigrupos do semigrupo monogénico infinito $\mathbb{N}$ (um em cada linha). (*iv*) Prova-se usando (*iii*) e o anti-isomorfismo$\widehat{\ }$. □

9.2 Automaticidade

Dado o conjunto finito A, e o subconjunto L de A^+, dizemos que L é *regular* se existir um autómato finito que o reconheça, e dizemos que L é *racional* se o pudermos obter a partir de subconjuntos finitos de A^* aplicando um número finitos vezes, $\cdot$ (multiplicação) e $*$ (operação estrela de Klenne). É sabido que as noções de "regular"e "racional"coincidem e podemos usá-las como sinónimos. Para sermos capazes de lidar com autómatos que aceitam pares de palavras e definam automaticamente semigrupos necessitamos de definir um novo alfabeto $A(2,\$) = ((A \cup \{\$\}) \times (A \cup \{\$\}))\backslash\{(\$,\$)\}$ em que $\$$ não é um símbolo de A (chamado símbolo completivo) e a função $\delta_A : A^* \times A^* \to A(2,\$)^*$ definido por

$$(a_1 \ldots a_m, b_1 \ldots b_n)\delta_A = \begin{cases} \epsilon & \text{se } 0 = m = n \\ (a_1, b_1) \ldots (a_m, b_m) & \text{se } 0 < m = n \\ (a_1, b_1) \ldots (a_m, b_m)(\$, b_{m+1}) \ldots (\$, b_n) & \text{se } 0 \leq m < n \\ (a_1, b_1) \ldots (a_n, b_n)(a_{n+1}, \$) \ldots (a_m, \$) & \text{se } m > n \geq 0. \end{cases}$$

Seja S um semigrupo e A um conjunto gerador finito para S com respeito a $\psi : A^+ \to S$. O par (A, L) é uma *estrutura automática para S (com respeito a ψ)* se

- L é um subconjunto regular de A^+ e $L\psi = S$,
- $L_= = \{(\alpha, \beta) : \alpha, \beta \in L, \alpha = \beta\}\delta_A$ é regular em $A(2,\$)^+$, e

- $L_a = \{(\alpha, \beta) : \alpha, \beta \in L, \alpha a = \beta\}\delta_A$ é regular em $A(2, \$)^+$ para cada $a \in A$,

em que $\alpha = \beta$ significa que α e β representam o mesmo elemento em S (i.e. $\alpha\psi = \beta\psi$). Dizemos que um semigrupo é *automático* se tiver uma estrutura automática. Para uma introdução mais detalhada ver [5].

Se (A, L) é uma estrutura automática para um semigrupo S então existe uma estrutura automática (A, K) tal que cada elemento de S tem uma única representação em K (ver [5, Proposição 5.4]); dizemos que (A, K) é uma *estrutura automática única* e que K é um *conjunto de formas normais únicas para* S.

Para definições alternativas de "Semigrupo Automático" ver [14].

Nesta subsecção iremos considerar automaticidade de subsemigrupos do monoide bicíclico e o nosso resultado principal é o seguinte:

Teorema 3.27. *Todos os subsemigrupos finitamente gerados do monoide bicíclico são automáticos.*

Um subsemigrupo finito de $\mathbf{B}$ é uma reunião finita de subsemigrupos de $\mathbb{N}$ e cópias de $\mathbf{B}$. Contudo, não sabemos se uma reunião finita de semigrupos automáticos é automática. Para provarmos o teorema anterior necessitaremos dos resultados seguintes, de [13]:

Proposição 3.28. *Seja S um semigrupo e T um subsemigrupo de S tais que o conjunto $S\backslash T$ é finito. Então S é automático se e só se T é automático.*

Lema 3.29. *Para quaisquer números $p, m \in \mathbb{N}_0$ com $p \leq m$, $d \in \mathbb{N}$ e conjuntos $I \subseteq \{0, \ldots, p-1\}$, $P \subseteq \{0, \ldots, d-1\}$ tais que $0 \in P$, cada um dos seguintes subconjuntos do monoide bicíclico é automático sempre que for um subsemigrupo:*

$$\begin{array}{ll} (i)\ \ \Lambda_{I,m,d}; & (ii)\ \ \widehat{\Lambda_{I,m,d}}; \\ (iii)\ \ \Sigma_{p,d,P} \cup \Lambda_{I,p,d}; & (iv)\ \ \Sigma_{p,d,P} \cup \widehat{\Lambda_{I,p,d}}. \end{array}$$

Demonstração. Note-se que embora os semigrupos (ii) e (iv) se obtenham de (i) e (ii), respectivamente, usando o anti-isomorfismo $\widehat{\ }$, a nossa noção de estrutura automática envolve multiplicação à direita e portanto não podemos simplesmente aplicar $\widehat{\ }$ para obter as estruturas automáticas pretendidas, assim, necessitamos de provar os quatro casos separadamente.

(i) Seja $i + u_i d = \min\{i + ud : i + ud \geq m\}$ para $i \in I$. Fixando $i_0 \in I$ e $u = u_{i_0}$ definimos a alfabeto

$$\Lambda = \bigcup_{i \in I} \{\lambda(i, 0), \ldots, \lambda(i, u-1)\}$$

e o homomorfismo

$$f : \Lambda^* \to \Lambda_{I,m,d}; \lambda(i,j) \mapsto c^i b^{i+(u_i+j)d}.$$

Definindo

$$L = \bigcup_{i\in I}(\bigcup_{j=0}^{u-1}\{\lambda(i,j)\lambda(i_0,0)^n : n \geq 0\})$$

é claro que L é uma linguagem regular e mostraremos que é um conjunto de formas normais únicas para $S = \Lambda_{I,m,d}$. Dado $s \in S$ podemos escrever $s = c^i b^{i+(u_i+k)d}$ para algum $i \in I$ e $k \geq 0$. Dividindo k por u obtemos $k = nu + j$ com $n \geq 0$ e $0 \leq j < u$, e assim a única palavra em L representando s é a palavra $\lambda(i,j)\lambda(i_0,0)^n$. Para provar que o par (Λ, L) é uma estrutura automática para S temos que provar apenas que as linguagens

$$L_{\lambda(k,l)} = \{(w_1, w_2)\delta : w_1, w_2 \in L, w_1\lambda(k,l) = w_2\}$$

são regulares para todo $\lambda(k,l) \in \Lambda$. Podemos escrever

$$\lambda(i,j)\lambda(i_0,0)^n\lambda(k,l) = c^i b^{i+(u_i+j)d+nud} c^k b^{k+(u_k+l)d} = c^i b^{i+(u_i+j+u_k+l)d+nud}$$

e dividindo $j + u_k + l$ por u obtemos $j + u_k + l = qu + r$ com $q \geq 0$ e $0 \leq r < u$ e obtemos assim

$$\lambda(i,j)\lambda(i_0,0)^n\lambda(k,l) = c^i b^{i+(u_i+r)d+(n+q)ud} = \lambda(i,r)\lambda(i_0,0)^{n+q},$$

em que $w = s$ com $w \in \Lambda^*$, $s \in S$ significa que w representa o elemento s (i.e. $wf = s$).

Temos portanto

$$L_{\lambda(k,l)} = \bigcup_{i\in I}(\bigcup_{j=0}^{u-1} Y_{k,l,i,j}) \tag{3.5}$$

em que

$$\begin{aligned} Y_{k,l,i,j} = \{ \quad & (\lambda(i,j)\lambda(i_0,0)^n,\ \lambda(i,r)\lambda(i_0,0)^{n+q})\delta : \\ & u_k + j + l = qu + r,\ 0 \leq r < u,\ n \geq 0\}. \end{aligned}$$

cada conjunto $Y_{k,l,i,j}$ é regular porque os números q e r são unicamente determinados fixando os números k, l, i e j. De facto, obtemos

$$Y_{k,l,i,j} = \{(\lambda(i,j), \lambda(i,r))\} \cdot \{(\lambda(i_0,0), \lambda(i_0,0))\}^* \cdot \{(\epsilon, \lambda(i_0,0)^q)\delta\}.$$

Logo $L_{\lambda(k,l)}$ é regular.

(ii) Definimos u_i $(i \in I)$, i_0, u e o alfabeto Λ tal como na demonstração de (i), mas agora o nosso homomorfismo é

$$f : \Lambda^* \to S;\ \lambda(i,j) \mapsto c^{i+(u_i+j)d} b^i$$

e a nossa linguagem regular é

$$L = \bigcup_{i \in I} (\bigcup_{j=0}^{u-1} \{\lambda(i_0,0)^n \lambda(i,j) : n \geq 0\}),$$

em que $S = \widehat{\Lambda_{I,m,d}}$. Novamente, L é um conjunto de formas normais únicas para S, como $\lambda(i_0,0)^n\lambda(i,j) = c^{i+(u_i+j)d+nud}b^i$, provaremos que as linguagens

$$L_{\lambda(k,l)} = \{(w_1, w_2)\delta : w_1, w_2 \in L, w_1\lambda(k,l) = w_2\}$$

são regulares para todo $\lambda(k,l) \in \Lambda$. Podemos escrever

$$\lambda(i_0,0)^n\lambda(i,j)\lambda(k,l) = c^{i+(u_i+j)d+nud}b^i c^{k+(u_k+l)d}b^k = c^{k+(u_k+j+u_i+l)d+nud}b^k$$

dividindo $j + u_i + l$ por u obtemos $j + u_i + l = qu + r$ com $q \geq 0$ e $0 \leq r < u$ e temos assim

$$\lambda(i_0,0)^n\lambda(i,j)\lambda(k,l) = c^{k+(u_k+r)d+(q+n)ud}b^k = \lambda(i_0,0)^{q+n}\lambda(k,r).$$

Temos portanto

$$\begin{aligned} L_{\lambda(k,l)} = \textstyle\bigcup_{i\in I}(\bigcup_{j=0}^{u-1}\{ \quad & (\lambda(i_0,0)^n\lambda(i,j), \lambda(i_0,0)^{n+q}\lambda(k,r))\delta : \\ & u_i + j + l = qu + r, 0 \leq r < u, n \geq 0\}) \end{aligned}$$

que é uma reunião finita de linguagens regulares e portanto é regular.

(iii) Seja $Z = \Lambda \cup \{x, y\} \cup \Gamma$, em que $\Lambda = \{\lambda_i : i \in I\}$ e $\Gamma = \{\gamma_r : r \in P\}$, seja um alfabeto e definimos

$$L = \bigcup_{i \in I} (\{\lambda_i x^u : u \geq 0\}) \cup \bigcup_{r \in P} (\{y^v \gamma_r x^u : u, v \geq 0\}),$$

que é um subconjunto regular de Z^+. Iremos provar que (Z, L) é uma estrutura automática (com unicidade) para o semigrupo $S = \Sigma_{p,d,P} \cup \Lambda_{I,p,d}$ com respeito a

$$f : Z^+ \to S;\ \ \lambda_i \mapsto c^i b^{i+u_i d},\ \gamma_r \mapsto c^{p+r}b^{p+r},\ x \mapsto c^p b^{p+d},\ y \mapsto c^{p+d}b^p$$

em que $i + u_i d = \min\{i + ud : i + ud \geq p\}$ para $i \in I$.

Para mostrar que cada elemento de S tem uma única representação em L basta observar que

$$\lambda_i x^u = c^i b^{i+(u_i+u)d} \quad (i \in I; u \geq 0), \quad y^v \gamma_r x^u = c^{p+r+vd} b^{p+r+ud} \quad (r \in P; u, v \geq 0).$$

Portanto, temos apenas que mostrar que $L_z = \{(w_1, w_2)\delta : w_1, w_2 \in L, w_1 z = w_2\}$ é regular para todo $z \in Z$.

Primeiro consideramos o caso em que $z = \lambda_t \in \Lambda$. Como $\Psi((\lambda_i x^u)f)$ e $\Psi((y^v \gamma_r x^u)f) \geq p > t = \Phi(\lambda_t f)$ obtemos

$$L_{\lambda_t} = \bigcup_{i \in I} \{(\lambda_i x^u, \lambda_i x^{u+u_t})\delta : u \geq 0\} \cup \bigcup_{r \in P} \{(y^u \gamma_r x^u, y^v \gamma_r x^{u+u_t})\delta : u, v \geq 0\}$$

que é uma linguagem regular.

Consideremos agora o caso em que $z = \gamma_t \in \Gamma$. Como para $u > 0$ temos $\Psi((\lambda_i x^u)f), \Psi((y^v \gamma_r x^u)f) \geq p + d > \Phi(\gamma_t f)$ obtemos assim

$$\begin{aligned} L_{\gamma_t} = \ & \textstyle\bigcup_{i \in I}(\{(\lambda_i x^u, \lambda_i x^u)\delta : u > 0\} \cup \{(\lambda_i, w)\delta : w \in L, \lambda_i \gamma_t = w\}) \cup \\ & \textstyle\bigcup_{r \in P}(\{(y^v \gamma_r x^u, y^v \gamma_r x^u)\delta : v \geq 0, u > 0\} \cup L_{(\gamma_t, r)}) \end{aligned}$$

em que

$$L_{(\gamma_t, r)} = \begin{cases} \{(y^u \gamma_r, y^u \gamma_r)\delta : u \geq 0\} & \text{caso } r \geq t \\ \{(y^u \gamma_r, y^u \gamma_t)\delta : u \geq 0\} & \text{caso contrário.} \end{cases}$$

Note-se que, para cada $i \in I$, o conjunto $\{(\lambda_i, w)\delta : w \in L, \lambda_i \gamma_t = w\}$ tem apenas um elemento porque L é um conjunto de formas normais únicas para S, e assim a linguagem L_{γ_t} é a reunião finita de linguagens regulares e portanto é regular. A linguagem L_x é claramente regular uma vez que temos $L_x = \{(w, wx)\delta : w \in L\}$. Finalmente, temos

$$\begin{aligned} L_y = \ & \textstyle\bigcup_{i \in I}(\{(\lambda_i x^u, \lambda_i x^{u-1})\delta : u > 0\} \cup \{(\lambda_i, w)\delta : w \in L, \lambda_i y = w\}) \cup \\ & \textstyle\bigcup_{r \in P}(\{(y^v \gamma_r x^u, y^v \gamma_r x^{u-1})\delta : v \geq 0, u > 0\} \cup \{(y^v \gamma_r, y^{v+1} \gamma_0)\delta : v \geq 0\}) \end{aligned}$$

porque, para $v \geq 0$, temos

$$(y^v \gamma_r)y = (c^{p+r+vd} b^{p+r})(c^{p+d} b^p) = c^{p+(v+1)d} b^p = y^{v+1} \gamma_0.$$

Novamente, para cada $i \in I$, o conjunto $\{(\lambda_i, w)\delta : w \in L, \lambda_i y = w\}$ é regular porque contém apenas um elemento, logo, L_y é também uma reunião finita de linguagens regulares e portanto é regular. Concluímos que S é automático.

(iv) Definimos o alfabeto Z tal como na prova na prova de (iii) e a nossa linguagem regular sobre Z^+ é agora

$$L = \bigcup_{i \in I}(\{y^v \lambda_i : v \geq 0\}) \cup \bigcup_{r \in P}(\{y^v \gamma_r x^u : u, v \geq 0\}).$$

Provaremos então que (Z, L) é uma estrutura automática (com unicidade) para o semigrupo $S = \Sigma_{p,d,P} \cup \widehat{\Lambda_{I,p,d}}$ com respeito a

$$f : Z^+ \to S; \quad \lambda_i \mapsto c^{i+u_i d} b^i, \ \gamma_r \mapsto c^{p+r} b^{p+r}, \ x \mapsto c^p b^{p+d}, \ y \mapsto c^{p+d} b^p$$

novamente com $i + u_i d = \min\{i + ud : i + ud \geq p\}$ para $i \in I$.

É mais uma vez claro que L é um conjunto formas normais únicas para S e mostraremos que a linguagens $L_z = \{(w_1, w_2)\delta : w_1, w_2 \in L, w_1 z = w_2\}$ são regulares para cada $z \in Z$. Começaremos por mostrar que, para todo $\lambda_t \in \Lambda$, temos

$$\begin{array}{rl} L_{\lambda_t} = & \bigcup_{i \in I} \{(y^v \lambda_i, y^{v+u_i} \lambda_t)\delta : v \geq 0\} \cup \\ & \bigcup_{r \in P} (\{(y^v \gamma_r x^u, y^v \gamma_r x^{u-u_t})\delta : v \geq 0, u \geq u_t\} \cup L_{(\lambda_t, r)} \cup \\ & \bigcup_{u=1}^{u_t - 1} \{(y^v \gamma_r x^u, y^{v+u_t-u-u_k} \lambda_k)\delta : v \geq 0, k = p + r + (u - u_t)d\}) \end{array}$$

em que

$$L_{(\lambda_t, r)} = \begin{cases} \{(y^v \gamma_r, y^v \lambda_t)\delta : v \geq 0\} & \text{caso } p + r \leq t + u_t d \\ \{(y^v \gamma_r, y^{v+u_t-u_k} \lambda_k)\delta : k = p + r - u_t d\} & \text{caso contário.} \end{cases}$$

Temos

$$y^v \lambda_i \lambda_t = c^{i+u_i d+vd} b^i c^{t+u_t d} b^t = c^{t+u_t d+(v+u_i)d} b^t = y^{v+u_i} \lambda_t.$$

Se $u \geq u_t$ então

$$y^v \gamma_r x^u \lambda_t = c^{p+r+vd} b^{p+r+ud} c^{t+u_t d} b^t = c^{p+r+vd} b^{p+r+(u-u_t)d} = y^v \gamma_r x^{u-u_t}.$$

Para $u \in \{1, \ldots, u_t - 1\}$ definimos $k = p + r + (u - u_t)d$ e obtemos

$$\begin{array}{rl} w & = y^v \gamma_r x^u \lambda_t = c^{p+r+vd} b^{p+r+ud} c^{t+u_t d} b^t = c^{p+r+vd} b^{p+r+(u-u_t)d} \\ & = c^{k+(v+u_t-u)d} b^k = c^{k+u_k d+(v+u_t-u-u_k)d} b^k. \end{array}$$

Como S é um semigrupo e $k < p$ temos $w \in \widehat{\Lambda_{I,p,d}}$, portanto, observando a definição de u_k, temos $v + u_t - u - u_k \geq 0$ e podemos escrever $w = y^{v+u_t-u-u_k} \lambda_k$. Consideremos agora a multiplicação de uma palavra da forma $y^v \gamma_r$ por λ_t e assim definimos $w = y^v \gamma_r \lambda_t = c^{p+r+vd} b^{p+r} c^{t+u_t d} b^t$. Se $p + r \leq t + u_t d$ então $w = c^{t+u_t d+vd} b^t = y^v \lambda_t$. Se $p + r > t + u_t d$ temos $w = c^{p+r+vd} b^{p+r-u_t d}$. Note-se que $u_t > 0$ porque $t < p$ e $t + u_t d \geq p$, portanto, $w \in \widehat{\Lambda_{I,p,d}}$. Assim, definindo $k = p + r - u_t d$ podemos escrever

$$w = c^{k+(v+u_t)d} b^k = c^{k+u_k d+(v+u_t-u_k)d} b^k$$

e, da definição de u_k, sai que $v + u_t - u_k \geq 0$, temos então $w = y^{v+u_t-u_k}\lambda_k$. Concluímos que L_{λ_t} pode ser definido como uma reunião finita de linguagens regulares e então é uma linguagem regular.

Facilmente se vê que

$$\begin{array}{rl} L_{\gamma_t} = & \bigcup_{i\in I}\{(y^v\lambda_i, y^{v+u_i}\gamma_t)\delta : v \geq 0\} \cup L_{(\gamma_t,r)} \\ & \bigcup_{r\in P}\{(y^v\gamma_r x^u, y^v\gamma_r x^u)\delta : u > 0, v \geq 0\} \end{array}$$

em que

$$L_{(\gamma_t,r)} = \begin{cases} \{(y^v\gamma_r, y^v\gamma_r)\delta : v \leq 0\} & \text{caso } r \geq t \\ \{(y^v\gamma_r, y^v\gamma_t)\delta : v \geq 0\} & \text{caso contrário} \end{cases}$$

é uma linguagem regular. A linguagem L_x é regular porque

$$L_x = \bigcup_{i\in I}\{(y^v\lambda_i, y^{u_i+v}\gamma_0 x)\delta : v \geq 0\} \cup \bigcup_{r\in P}\{(y^v\gamma_r x^u, y^v\gamma_r x^{u+1})\delta : u, v \geq 0\}$$

e tendo em conta que

$$\begin{array}{rl} L_y = & \bigcup_{i\in I}\{(y^v\lambda_i, y^{v+u_i+1}\gamma_0)\delta : v \geq 0\} \cup \\ & \bigcup_{r\in P}(\{(y^v\gamma_r x^u, y^v\gamma_r x^{u-1})\delta : v \geq 0, u > 0\} \cup \{(y^v\gamma_r, y^{v+1}\gamma_0)\delta : v \geq 0\}) \end{array}$$

L_y é também uma linguagem regular. Concluímos assim que (Z, L) é uma estrutura automática para S. □

Demonstração do Teorema 3.27 Sabemos da subsecção anterior que qualquer subsemigrupo finitamente gerado ou é um subconjunto finito da diagonal, e portanto é automático, ou tem uma das formas:

$$\begin{array}{l} F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P},\ F_D \cup F \cup \widehat{\Lambda_{I,p,d}} \cup \Sigma_{p,d,P}, \\ F_D \cup F \cup \Lambda_{I,p,d},\ F_D \cup F \cup \widehat{\Lambda_{I,p,d}} \end{array}$$

em que $I \subseteq \{q, q+1, \ldots, p-1\}$ para alguns $q, p \in \mathbb{N}_0$, e os conjuntos F e F_D são finitos. Em cada um dos casos podemos remover o conjunto finito $F_D \cup F$ do nosso subsemigrupo, porque estamos na verdade a intersectá-lo com o conjunto $S_{q,p} \cup \Sigma_p$, que é, pelo Teorema 3.1, também um subsemigrupo. Assim, cada subsemigrupo finitamente gerado S de $\mathbf{B}$ tem um subsemigrupo U tal que $S\backslash U$ é finito e, pelo Lema anterior, é automático. Da Proposição 3.28, tiramos que S é também automático. □

9.3 Apresentação Finita

Seja A um alfabeto e $R \subseteq A^+ \times A^+$ uma relação em A^+. Dizemos que o semigrupo S é definido pela apresentação $\langle A \mid R\rangle$ se $S \cong A^+/\rho$ em que $\rho \subseteq A^+ \times A^+$ é

a mais pequena congruência em A^+ que contém R. Dado um semigrupo S com a apresentação $\langle A \mid R\rangle$, para duas palavras $w, v \in A^+$ escrevemos $w \to^* v$, e dizemos que $w = v$ é uma *congruência de* R (ou que a palavra w *poder ser reduzida a* v aplicando relações de R), com o significado de, ou $w \equiv v$ ou que existe uma sequência de palavras $w \equiv w_1, w_2, \ldots, w_n \equiv v$ em que $w_i \equiv w_i' v_i w_i''$, com $w_i', w_i'' \in A^*$ e $v_i \in A^+$ $(i = 1, \ldots, n)$ tais que ou $(v_i, v_{i+1}) \in R$ ou $(v_{i+1}, v_i) \in R$ para todo $(i = 1, \ldots, n-1)$.

Sabemos que, dado um semigrupo S gerado por um conjunto A e dado um conjunto $R \subseteq A^+ \times A^+$, o par $\langle A \mid R\rangle$ é uma apresentação para S, se e só se S satisfizer todas as relações de R ($u = v$ mantém-se em S para todo $(u, v) \in R$) e se $u = v$ se mantém em S $(u, v \in A^+)$ então $u = v$ é uma consequência de R. Usaremos a seguinte consequência deste facto:

Proposição 3.30. *Seja S um semigrupo gerado pelo conjunto A, seja $R \subseteq A^+ \times A^+$ e seja $L \subseteq A^+$ um conjunto de formas normais únicas para S. Se se verificarem as seguintes condições então $\langle A \mid R\rangle$ é uma apresentação para S;*

(*i*) *S satisfaz todas as condições de R;*

(*ii*) *qualquer palavra $w \in A^+$ pode ser reduzida à correspondente forma normal única em L usando as relações de R.*

Dizemos que um semigrupo S é *finitamente apresentado* se existir uma apresentação $\langle A \mid R\rangle$ para S em que A e R são conjuntos finitos. Para mais detalhes sobre apresentações de semigrupos aconselhamos [24].

Na subsecção anterior a Proposição 3.28 permite-nos remover subconjuntos finitos dos semigrupos quando consideramos a automaticidade. Temos um resultado similar para a apresentação finita, provado em [33]:

Proposição 3.31. *Seja S um semigrupo e T um subsemigrupo de S tal que $S \backslash T$ é finito. Então S é finitamente apresentado se e só se T for finitamente apresentado.*

Seguidamente apresentamos o resultado mais importante desta subsecção:

Teorema 3.32. *Todos os subsemigrupos finitamente gerados do monoide bicíclico são finitamente apresentados.*

Para a demonstração deste teorema necessitaremos do resultado seguinte:

Lema 3.33. *Para quaisquer números* $p, m \in \mathbb{N}_0$ *com* $p \leq m$, $d \in \mathbb{N}$ *e conjuntos*

$$I \subseteq \{0, \ldots, p-1\}, \quad P \subseteq \{0, \ldots, d-1\}$$

tais que $0 \in P$, *cada um dos seguintes subconjuntos de* $\boldsymbol{B}$ *é finitamente apresentado sempre que for um semigrupo:*

$$(i)\ \Lambda_{I,m,d}; \qquad (ii)\ \Lambda_{I,p,d} \cup \Sigma_{p,d,P}.$$

Demonstração. (i) Consideremos a estrutura automática (Λ, L) obtida na demonstração do Lema 3.29 (i), que nos dá um conjunto gerador finito e um conjunto formas normais únicas para $\Lambda_{I,m,d}$. Provaremos que $< \Lambda \mid R >$ é uma apresentação finita para T, em que R consiste nas seguintes relações:

$$\lambda(i,j)\lambda(k,l) = \lambda(i,r)\lambda(i_0,0)^q \text{ em que } \begin{array}{l} j + u_k + l = qu + r, \quad 0 \leq r < u \\ (i,k \in I, j,l \in \{0,\ldots,u-1\}). \end{array}$$

Que se verificam estas relações sai-nos de 3.5, na demonstração do Lema 3.29. Provaremos que qualquer palavra $w \in \Lambda^+$ pode ser reduzida a uma palavra de L, através das relações de R, usando indução sobre o comprimento $|w|$ da palavra w. Se $|w| = 1$ então $w \in L$, pela definição de L. Se $|w| = 2$ então $w = \lambda(i,j)\lambda(k,l)$ e portanto

$$w \to^* \lambda(i,r)\lambda(i_0,0)^q \in L, \quad j + u_k + l = qu + r \quad (0 \leq r < u),$$

que é uma relação em R. Seja $n \geq 2$ e suponhamos que qualquer palavra w, tal que $|w| \leq n$, pode ser reduzida a uma palavra de L, usando relações de R. Seja $w \in \Lambda^+$ com $|w| = n+1$. Temos $w = \lambda(i_1,j_1)\ldots\lambda(i_n,j_n)\lambda(i_{n+1},j_{n+1})$. Podemos reduzir $\lambda(i_n,j_n)\lambda(i_{n+1},j_{n+1})$ obtendo

$$w \to^* \lambda(i_1,j_1)\ldots\lambda(i_{n-1},j_{n-1})\lambda(i_n,r)\lambda(i_0,0)^q$$

em que

$$j_n + u_{i_{n+1}} + j_{n+1} = qu + r \quad (0 \leq r < u).$$

Fazendo $w' = \lambda(i_1,j_1)\ldots\lambda(i_{n-1},j_{n-1})\lambda(i_n,r)$ temos $|w'| = n$ e, usando a hipótese da indução, obtemos $w' \to^* \lambda(i,j)\lambda(i_0,0)^m \in L$ para algum $i \in I$, $j \in \{0,\ldots,u-1\}$, $m \in \mathbb{N}_0$, o que implica $w \to^* \lambda(i,j)\lambda(i_0,0)^{m+q} \in L$.

(ii) Usaremos a estrutura automática (Z, L) obtida na demonstração do Lema 3.29 (iii) para provar que $T = \Sigma_{p,d,P} \cup \Lambda_{I,p,d}$ é finitamente apresentado. Mostraremos

que $< Z \mid R >$ é uma apresentação finita para T, definindo R como o seguinte conjunto de relações:

$$x = \gamma_0 x \tag{3.6}$$
$$y = y\gamma_0 \tag{3.7}$$
$$\lambda_i\lambda_j = \lambda_i x^{u_j} \quad (i,j \in I) \tag{3.8}$$
$$x\lambda_i = x^{1+u_i} \quad (i \in I) \tag{3.9}$$
$$y\lambda_i = yx^{u_i} \quad (i \in I) \tag{3.10}$$
$$\gamma_r\lambda_i = \gamma_r x^{u_i} \quad (r \in P, i \in I) \tag{3.11}$$
$$xy = \gamma_0 \tag{3.12}$$
$$\lambda_i y = \lambda_j \quad (i \in I, u_i > 1, j = p + d - u_i d) \tag{3.13}$$
$$\lambda_i y = \gamma_0 \quad (i \in I, u_i = 1) \tag{3.14}$$
$$\gamma_r y = y \quad (r \in P) \tag{3.15}$$
$$x\gamma_r = x \quad (r \in P) \tag{3.16}$$
$$\lambda_i\gamma_r = \lambda_i \quad (i \in I, r \in P, i + u_i d \geq p + r) \tag{3.17}$$
$$\lambda_i\gamma_r = \lambda_j \quad (i \in I, r \in P, i + u_i d < p + r, j = p + r - u_i d) \tag{3.18}$$
$$\gamma_r\gamma_t = \gamma_r \quad (r \geq t) \tag{3.19}$$
$$\gamma_r\gamma_t = \gamma_t \quad (r < t) \tag{3.20}$$

Para vermos que uma relação se verifica basta-nos provar que cada um dos membros corresponde à mesma palavra em $\{c^i b^j : i,j \geq 0\}$. Provaremos que se verificam as relações 3.13, 3.14, 3.19 e 3.20, as restantes facilmente se verificam.

Começamos pelas relações 3.13 e 3.14. Observamos que, pela definição de u_i, temos $\lambda_i y = c^i b^{i+u_i d} c^{p+d} b^p = c^{p+d-u_i d} b^p$. Se $u_i = 1$ então $\lambda_i y = c^p b^p = \gamma_0$, logo verifica-se 3.14. Se $u_i > 1$ então $p+d-u_i d < p$, e assim, definido $j = p+d-u_i d$, temos $\lambda_i y = c^j b^{j+(u_i-1)d} \in \Lambda_{I,p,d}$. Mas temos $j + (u_i - 1)d = p$ o que implica, da definição de u_j, que $u_i - 1 = u_j$, o que significa que $\lambda_i y = \lambda_j$, logo verifica-se também 3.13.

Para provar as relações 3.19 e 3.20, comecemos por escrever

$$\lambda_i\gamma_r = c^i b^{i+u_i d} c^{p+r} b^{p+r}.$$

Caso $i+u_i d \geq p+r$ então $\lambda_i\gamma_r = c^i b^{i+u_i d} = \lambda_i$, verificando-se 3.19. Caso contrário, temos $\lambda_i\gamma_r = c^{p+r-u_i d} b^{p+r} \in \Lambda_{I,p,d}$ porque $u_i > 0$. Definido $j = p+r-u_i d$ temos $\lambda_i\gamma_r = c^j b^{j+u_i d}$ e, como $j + u_i d = p + r < p + d$ e usando a definição de u_j, temos que ter $u_i = u_j$, o que implica $\lambda_i\gamma_r = \lambda_j$, assim, verifica-se também 3.20.

Vamos agora provar que qualquer palavra $w \in Z^+$ pode ser reduzida a uma palavra em L, usando as nossas relações, através da indução no comprimente de w. Se $|w| = 1$ então, ou $w \in L$, ou w pode ser reduzida a uma palavra em L, usando as relações de 3.6 ou 3.7.

Consideremos agora palavras de comprimento 2:

- a palavra $\lambda_i\lambda_t$ reduz-se a $\lambda_i x^{u_t} \in L$, usando (3.8);
- $\lambda_i x \in L$;
- $\lambda_i y$ ou se reduz a $\gamma_0 \in L$ usando, (3.14), ou a $\lambda_j \in L$, para algum j, usando a relação (3.13);
- $\lambda_i\gamma_r$ reduz-se a $\lambda_j \in L$, para algum j, usando as relações (3.17) ou (3.18);
- xx reduz-se a $\gamma_0 x^2 \in L$, usando (3.6);
- xy reduz-se a $\gamma_0 \in L$ usando a relação (3.12);
- $x\lambda_i$ reduz-se a $\gamma_0 x^{1+u_i} \in L$ usando as relações (3.9) e (3.6);
- $x\gamma_t$ reduz-se a $\gamma_0 x \in L$ usando as relações (3.16) e (3.6);
- yx reduz-se a $y\gamma_0 x \in L$ usando (3.6);
- yy reduz-se a $y^2\gamma_0 \in L$ usando (3.7);
- $y\lambda_i$ reduz-se a $y\gamma_0 x^{u_i} \in L$ usando (3.10) e (3.7);
- $y\gamma_t \in L$;
- $\gamma_i x \in L$;
- $\gamma_i y$ reduz-se a $y\gamma_0 \in L$ usando (3.15) e (3.7);
- $\gamma_i\lambda_t$ reduz-se a $\gamma_i x^{u_t} \in L$ usando (3.11);
- $\gamma_i\gamma_r$ reduz-se a $\gamma_j \in L$, para algum j, usando (3.19) ou (3.20).

No próximo passo da indução usaremos o facto de que, se a palavra w pertencer a L então, da definição de L, wx^n também pertence a L para qualquer $n \in \mathbb{N}_0$. Seja $n \geq 2$ e suponhamos que todas as palavras $w \in Z^+$ com $|w| \leq n$ se podem reduzir a uma palavra de L. Seja $w \in Z^+$ uma palavra de comprimento $n+1$. Então, temos $w = w_1 g_1 g_2$ com $w_1 \in Z^+$ e $g_1, g_2 \in Z$. Vamos considerar todos os pares possíveis de geradores $g_1, g_2 \in Z$ e provar que em todos os casos w se reduz a uma palavra de L, usando as relações.

Caso 1: $g_1g_2 \in \{\lambda_i y, \lambda_i\gamma_t, xy, x\gamma_t, \gamma_t y, \gamma_t\gamma_i\}$. Nestes casos podemos aplicar uma das relações para reduzir g_1g_2 a um gerador g. E depois podemos aplicar a hipótese indutiva para reduzir w_1g a uma palavra de L;

Caso 2: $g_1g_2 \equiv g_1x$. Nestes casos podemos reduzir w_1g_1 à palavra $w_2 \in L$, usando a hipótese indutiva, e portanto podemos reduzir w a $w_2x \in L$;

Caso 3: $g_1g_2 \equiv \lambda_i\lambda_t$. Usando a relação (3.8), temos $w \to^* w_1\lambda_i x^{u_t}$ e como $|w_1\lambda_i| = n$, usando a hipótese indutiva obtemos $w_1\lambda_i \to^* w_2 \in L$ e portanto, $w \to^* w_2x^{u_t} \in L$;

Caso 4: $g_1g_2 \equiv x\lambda_t$. Usando a relação (3.9) obtemos $w \to^* w_1x^{1+u_t}$. Tendo em conta que $|w_1| \leq n$, usando a hipótese, podemos escrever $w_1 \to^* w_2 \in L$ e assim $w \to^* w_1x^{1+u_t} \to^* w_2x^{1+u_t} \in L$;

Caso 5: $g_1g_2 \equiv y\lambda_t$. Usando a relação (3.10), reduzimos $y\lambda_t$ a yx^{u_t}. Podemos aplicar a hipótese indutiva a w_1y para obter $w_1y \to^* w_2 \in L$ o que implica $w \to^* w_2x^{u_t} \in L$;

Caso 6: $g_1g_2 \equiv yy$. Começamos por reduzir w_1y a uma palavra $w_2 \in L$, usando a hipótese indutiva. Podemos ter $w_2 \equiv \lambda_i x^u$ ou $w_2 \equiv y^v\gamma_r x^u$. Se $w_2 \equiv \lambda_i$ então $w \to^* \lambda_i y$, e aplicando as relações (3.13) ou (3.14) reduzimo-la a uma palavra em L. Se $w_2 \equiv \lambda_i x$ então $w \to^* \lambda_i xy \to^* \lambda_i\gamma_0$, aplicando a relação (3.12). Assim, aplicando agora as relações (3.17) ou (3.18), w reduz-se a uma palavra de L. Se $w_2 \equiv \lambda_i x^u$ com $u > 1$ então

$$w \to^* \lambda_i x^{u-1}xy \to^* \lambda_i x^{u-2}x\gamma_0 \to^* \lambda_i x^{u-1} \in L,$$

aplicando as relações (3.12) e (3.16). Se $w_2 \equiv y^v\gamma_r$ então

$$w \to^* y^v\gamma_r y \to^* y^v y \to^* y^{v+1}\gamma_0 \in L,$$

usando as relações (3.15) e (3.7). Se $w_2 \equiv y^v\gamma_r x$ então $w \to^* y^v\gamma_r xy$ e podemos aplicar (3.12) para reduzir xy a γ_0. Então podemos reduzir $\gamma_r\gamma_0$ a γ_r, aplicando a relação (3.19), e portanto $w \to^* y^v\gamma_r \in L$. Podemos ter $w_2 \equiv y^v\gamma_r x^u$ com $u > 1$ e assim,

$$w \to^* y^v\gamma_r x^{u-1}xy \to^* y^v\gamma_r x^{u-2}x\gamma_0 \to *y^v\gamma_r x^{u-1} \in L$$

usando as relações (3.12) e (3.16).

Caso 7: $g_1g_2 \equiv y\gamma_t$. Começamos por reduzir w_1y à palavra $w_2 \in L$. Pode ser $w_2 \equiv \lambda_i x^u$ ou $w_2 \equiv y^v\gamma_r x^u$. Se $w_2 \equiv \lambda_i$ então $w \to^* \lambda_i y$ e, aplicando a relação (3.13) ou (3.14), podemos reduzir w a um gerador que pertence a L. Se $w_2 \equiv \lambda_i x^u$ com $u > 0$ então, aplicando (3.16) dando $w \to^* \lambda_i x^u\gamma_t \to^* \lambda_i x^u \in L$. Se $w_2 \equiv y^v\gamma_r$ então $w \to^* y^v\gamma_r\gamma_t$, aplicando as relações (3.19) ou (3.20) obtemos $w \to^* y^v g \in L$ com $g \in \{\gamma_r, \gamma_t\}$. E por fim, se $w_2 \equiv y^v\gamma_r x^u$ com $u > 0$ então temos $w \to^* y^v\gamma_r x^u\gamma_t \to^* y^v\gamma_r x^u \in L$, usando a relação (3.16).

Caso 8: $g_1g_2 \equiv \gamma_t\lambda_i$. Aplicando a relação (3.11), obtemos $\gamma_t\lambda_i \to^* \gamma_t x^{u_i}$. Como $|w_1\gamma_t| \leq n$, usando a hipótese, temos $w_1\gamma_t \to^* w_2 \in L$ e portanto $w \to^* w_2x^{u_i} \in L$.

□

Demonstração do Teorema 3.32 Sabemos já que um subsemigrupo finitamente gerado ou é um subconjunto da diagonal, portanto é finitamente apresentado, ou tem uma das seguintes formas:

$$F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P},\ F_D \cup F \cup \widehat{\Lambda_{I,p,d}} \cup \Sigma_{p,d,P},$$
$$F_D \cup F \cup \Lambda_{I,p,d},\ F_D \cup F \cup \widehat{\Lambda_{I,p,d}}$$

em que $I \subseteq \{q, q+1, \ldots, p-1\}$ para alguns $q, p \in \mathbb{N}_0$, e para conjuntos F e F_D finitos. Podemos considerar, sem perda de generalidade, só os subsemigrupos da forma

$$F_D \cup F \cup \Lambda_{I,p,d} \cup \Sigma_{p,d,P}, \quad F_D \cup F \cup \Lambda_{I,p,d}$$

(os outros dois são anti-isomorfos a estes). Em ambos casos podemos remover o conjunto finito $F_D \cup F$ do nosso subsemigrupo e continuamos com um subsemigrupo. Assim, em ambos os casos, o nosso subsemigrupo S tem um subsemigrupo U tal que $S\backslash U$ é finito, que, pelo Lema 3.33, é finitamente apresentado. Então, pela Proposição 3.31, S é também finitamente apresentado. □

9.4 Residualmente finitos

Dizemos que um semigrupo S é *residualmente finito* se, para quaisquer dois elementos $s_1, s_2 \in S$, existe um semigrupo finito F e um homomorfismo $\phi : S \to F$ que separa s_1 e s_2 (tal que $s_1\phi \neq s_2\phi$). Consideremos o seguinte resultado:

Teorema 3.34. *Um semigrupo do monoide bicíclico* $\boldsymbol{B}$ *é residualmente finito se e só se não for bilateral.*

DEMONSTRAÇÃO. Mostremos primeiro que um semigrupo bilateral não é residualmente finito. De facto, um semigrupo bilateral S contém um subconjunto da forma $X = \{c^{p+ud}b^{p+vd};\ u, v \geq 0\}$, que é um subsemigrupo isomorfo ao monoide bicíclico; a função $\psi : \mathbf{B} \to X;\ c^u b^v \mapsto c^{p+ud}b^{p+vd}$ é claramente um isomorfismo. Tendo em conta que $\mathbf{B}$ não é residualmente finito então, S também não é residualmente finito (ver [25]).

Mostraremos agora que um subsemigrupo S contido em U (um semigrupo superior ou um subconjunto da diagonal) é residualmente finito. Seja $\alpha = c^i b^j$ e $\beta = c^k b^l$ dois elementos arbitrários em S. Tomando $p \geq \max(j, l)$ o conjunto $S_p = S \cap I_p$ é um ideal de S. Assim, o homomorfismo de Rees $\phi : S \to (S \backslash S_p) \cup \{0\}$ separa α e β, e $S \backslash S_p \cup \{0\}$ é finito, porque $S \backslash S_p \subseteq T_{0,p}$. Por analogia, qualquer subsemigrupo contido em $\widehat{U}$ é residualmente finito. □

Este teorema tem a seguinte formulação equivalente:

Teorema 3.35. *Um semigrupo do monoide bicíclico $\boldsymbol{B}$ é residualmente finito se e só se não contiver cópias de $\boldsymbol{B}$.*

Capítulo 4

GENERALIZAÇÕES DO MONOIDE BICÍCLICO

Neste capítulo tratamos generalizações do monoide bicíclico, em particular o monoide policíclico ([26]), fazemos ainda um pequena introdução às extensões de Bruck-Reilly com o intuito as relacionar com o monoide bicíclico ([2]) e fazemos uma breve referência a uma outra generalização do monoide bicíclico, de Celia L. Adair ([1]).

1 Monoide Policíclico

Nesta secção, tratamos monoides policíclicos. Estes foram introduzidos por Nivat e Perrot [30] como generalizações do monoide bicíclico.

Relembrando, que o monoide bicíclico pode ser representado em termos da função sucessor de números naturais (ver início do capítulo 2). Generalizando, se X for um qualquer conjunto isomorfo a um seu subconjunto próprio Y, através do isomorfismo $\theta : X \to Y$, então, as bijecções parciais θ e θ^{-1} em $I(X)$ geram um submonoide isomorfo ao monoide bicíclico. Assim, o monoide bicíclico surge-nos em contextos em que a estrutura é isomorfa a uma subestrutura própria. Para generalizar, começamos por considerar propriedades análogas no conjunto de Cantor.

O conjunto de Cantor, $\mathcal{C}$, é um subconjunto da linha real obtida do seguinte modo: Seja $F_1 = [0, 1]$, o intervalo unitário fechado e $F_2 = F_1 \backslash [\frac{1}{3}, \frac{2}{3}]$. Seja agora, $F_3 = F_2 \backslash ([\frac{1}{9}, \frac{2}{9}] \cup [\frac{7}{9}, \frac{8}{9}])$; o processo continua removendo em cada fase o terço central de cada intervalo restante. Definimos $\mathcal{C} = \bigcap_{i=0}^{\infty} F_i$.

Uma propriedade importante do conjunto de Cantor é que este é isomorfo a uma

união disjunta de duas cópias de si próprio. Observe-se primeiro que

$$\mathcal{C} = ([0, \frac{1}{3}] \cap \mathcal{C}) \cup ([\frac{2}{3}, 1] \cap \mathcal{C})$$

é uma reunião disjunta. Defina-se dois elementos de $I(\mathcal{C})$ da seguinte forma:

$$b : [0, \frac{1}{3}] \cap \mathcal{C} \to \mathcal{C} \quad \text{em que} \quad x \mapsto 3x$$

e

$$c : [\frac{2}{3}, 1] \cap \mathcal{C} \to \mathcal{C} \quad \text{em que} \quad x \mapsto 3x - 2.$$

Os elementos b e c geram um submonoide inverso de $I(\mathcal{C})$ que verifica as propriedades de auto-semelhança do conjunto de Cantor. No monoide inverso $I(\mathcal{C})$ verificam-se as equações $bb^{-1} = 1$ e $cc^{-1} = 1$, uma vez que a imagem de cada aplicação é todo o conjunto de Cantor. E ainda, $b^{-1}bc^{-1}c = 0$, porque, as funções têm domínios disjuntos. Esta equação é equivalente a $bc^{-1} = 0$.

Este exemplo motiva a seguinte definição. Para $n \geq 2$, o monoide policíclico em n geradores P_n é um semigrupo com zero com a seguinte apresentação:

$$P_n = \langle p_1, \ldots, p_n, p_1^{-1}, \ldots, p_n^{-1} : \ p_i p_i^{-1} = 1, \ p_i p_j^{-1} = 0 \ \text{ com } \ i \neq j \rangle.$$

Denotamos o monoide policíclico com um número infinito numerável de geradores por P_∞.

1.1 Propriedades do Monoide Policíclico

O monoide bicíclico, tal como já vimos, pode ser representado por bijecções parciais nos números naturais. Uma representação similar pode ser obtida para monóides policíclicos através de bijecções parciais sobre monóides livres. Seja $\Sigma = \{x_1, \ldots, x_n\}$. Definindo a função $\alpha_i : \Sigma^* \to \Sigma^*$ por $\alpha_i(u) = x_i u$, que tem domínio Σ^* e imagem $x_i\Sigma^*$. Podemos ver α_i como um elemento de $I(\Sigma^*)$. Denotemos por B_n o submonoide inverso de $I(\Sigma^*)$ gerado por α_i. Note-se que $\alpha_i^{-1}\alpha_i = 1$, a função identidade em $I(\Sigma^*)$, em que, se $i \neq j$ então $\alpha_i^{-1}\alpha_i = 0$, a função vazia em Σ^*. Definindo a função $\theta : P_n \to B_n$ por $\theta(p_i^{-1}) = \alpha_i$ e $\theta(p_i) = \alpha_i^{-1}$. Então, pela Proposição 1.70, B_n é uma imagem homomorfa de P_n.

No resultado seguinte, diremos que dois elementos de um semigrupo livre com zero são "equivalentes"se forem iguais em P_n; escrevemos "$u \equiv v$". Para uma sequência $p_{i_1} \ldots p_{i_m}$ definimos $(p_{i_1} \ldots p_{i_m})^{-1}$ como sendo $p_{i_m}^{-1} \ldots p_{i_1}^{-1}$.

Proposição 4.1. *P_n é isomorfo a B_n.*

DEMONSTRAÇÃO. Facilmente verificamos que todo elemento de P_n, diferente de zero, é equivalente a uma variável da forma $u^{-1}v$ em que $u, v, \in \{p_1, \ldots, p_n\}^*$.

Para provarmos que esta representação é única necessitamos do seguinte resultado: no semigrupo B_n, se

$$(\alpha_{i_1} \ldots \alpha_{i_m})(\alpha_{j_1} \ldots \alpha_{j_n})^{-1} = (\alpha_{k_1} \ldots \alpha_{k_p})(\alpha_{l_1} \ldots \alpha_{l_q})^{-1}$$

então $m = p$, $n = q$,

$$\alpha_{i_1} = \alpha_{k_1}, \ldots, \alpha_{i_m} = \alpha_{k_p} \quad \text{e} \quad \alpha_{j_1} = \alpha_{l_1}, \ldots, \alpha_{j_n} = \alpha_{l_q}.$$

Para vermos isto, observemos que o elemento

$$\alpha = \alpha_{i_1} \ldots \alpha_{i_m}$$

de B_n tem domínio Σ^* e imagem $x_{i_1} \ldots x_{i_m}\Sigma^*$, e que o elemento

$$\beta = (\alpha_{j_1} \ldots \alpha_{j_n})^{-1}$$

tem imagem Σ^* e domínio $x_{j_n} \ldots x_{j_1}\Sigma^*$. Logo, $\alpha\beta$ tem domínio $x_{j_n} \ldots x_{j_1}\Sigma^*$ e imagem $x_{i_1} \ldots x_{i_m}\Sigma^*$. Assim, elementos de B_n da forma

$$(\alpha_{i_1} \ldots \alpha_{i_m})(\alpha_{j_1} \ldots \alpha_{j_n})^{-1}$$

são unicamente determinados pelos seus domínios e imagens.

Podemos agora demonstrar que todo elemento de P_n, diferente de zero, é equivalente a uma única variável da forma $u^{-1}v$ em que $u, v, \in \{p_1, \ldots, p_n\}^*$. Suponhamos que $u^{-1}v \equiv x^{-1}y$, então, $\theta(u^{-1}v) = \theta(x^{-1}y)$ em B_n. Logo, $\theta(u)^{-1}\theta(v) = \theta(x)^{-1}\theta(y)$. Agora basta-nos usar o resultado anterior.

É agora claro que o homomorfismo sobrejectivo de P_n em B_n é injectivo. □

Para descrever a forma do produto em P_n, deveremos generalizar a operação monus introduzida no Capítulo 2.

Seja $x, y \in \{x_1, \ldots, x_n\}^*$, definamos

$$xy^{-1} = \begin{cases} u & \text{caso } y = ux \\ 1 & \text{caso contrário} \end{cases}$$

e

$$x^{-1}y = \begin{cases} v & \text{caso } y = xv \\ 1 & \text{caso contrário.} \end{cases}$$

O expoente "-1" é aqui utilizado no *cancelamento* de palavras e deve ser cuidadosamente distinguido do seu uso nos semigrupos inversos. Embora potencialmente confuso, o contexto torna, geralmente claro, qual dos casos se trata. As propriedades básicas da variável de cancelamento são dadas a seguir:

Lema 4.2. *Seja* $x, y, u, v \in \{x_1, \ldots, x_n\}^*$.

(1) $x(x^{-1}y) = y$ *se e só se* x *for um prefixo de* y.

(2) $(yx^{-1})x = y$ *se e só se* x *for um sufixo de* y.

(3) *O conjunto* $\Sigma^* u \cap \Sigma^* v$ *é diferente do vazio quando* u *é um sufixo de* v *ou* v *é um sufixo de* u. *Quando este conjunto for diferente do vazio temos* $(vu^{-1})u = (uv^{-1})v$, *e*

$$\Sigma^* u \cap \Sigma^* v = \Sigma^*(vu^{-1})u = \Sigma^*(uv^{-1})v.$$

(4) *O conjunto* $u\Sigma^* \cap v\Sigma^*$ *é diferente do vazio quando* u *é um prefixo de* v *ou* v *é um prefixo de* u. *Quando este conjunto for diferente do vazio temos* $v(v^{-1}u) = u(u^{-1}v)$, *e*

$$u\Sigma^* \cap v\Sigma^* = v(v^{-1}u)\Sigma^* = u(u^{-1}v)\Sigma^*.$$

Demonstração.

(1) Se $x(x^{-1}y) = y$, então é óbvio que x é um prefixo de y. Reciprocamente, suponhamos que x é um prefixo de y então $y = xu$, para algum u. Por definição, $u = x^{-1}y$. Logo, $x(x^{-1}y) = y$.

(2) Tem demonstração análoga à de (1).

(3) Das propriedades de monoides livres, facilmente se verifica que $\Sigma^* u \subseteq \Sigma^* v$ é diferente do vazio precisamente quando u é um sufixo de v ou v um sufixo de u. Suponhamos que u é um sufixo de v, então, por (2), $v = (vu^{-1})u$ e $(uv^{-1})v = 1v = v$. É claro que $\Sigma^* v \subseteq \Sigma^* u$ e portanto $\Sigma^* u \cap \Sigma^* v = \Sigma^* v$. O caso em que v é um sufixo de u demonstra-se de modo análogo.

(4) Tem demonstração análoga à de (3).

□

Com esta notação podemos agora obter um descrição sucinta da multiplicação em monoides policíclicos.

Lema 4.3. *Seja* $x^{-1}y$ *e* $u^{-1}v$ *dois elementos de* P_n*. O seu produto é diferente de zero quando* y *é um sufixo de* u *ou* u *um sufixo de* y*; isto é, quando a intersecção* $\Sigma^* y \cap \Sigma^* u$ *for diferente do vazio. Se* $(x^{-1}y)(u^{-1}v) \neq 0$ *então*

$$(x^{-1}y)(u^{-1}v) = ((uy^{-1})x)^{-1}((yu^{-1})v).$$

Demonstração. Consideremos primeiro todos os produtos da forma yu^{-1} em que $y, u \in \Sigma^*$. Suponhamos que y é um sufixo de u, então, $u = wy$ para algum $w \in \Sigma^*$, e portanto, $yu^{-1} = yy^{-1}w^{-1} = w^{-1}$. Se por outro lado, u for um sufixo de y, então, $y = wu$ para algum $w \in \Sigma^*$, e $yu^{-1} = wuu^{-1} = w$. Em qualquer um dos casos o produto é diferente de zero.

Suponhamos agora que nem y é sufixo de u nem u é sufixo de y. Então, existe $v \in \Sigma^*$ tal que $y = y_1 v$ e $u = u_1 v$ e as últimas letras de y_1 e u_1 são diferentes. Logo, $yu^{-1} = 0$, o que é um absurdo.

Consideremos agora o produto $(x^{-1}y)(u^{-1}v)$. Dos cálculos anteriores sabemos que é suficiente considerar o caso em que y é um sufixo de u ou vice-versa. Suponhamos que y é sufixo de u, então,

$$(x^{-1}y)(u^{-1}v) = x^{-1}w^{-1}v = (wx)^{-1}v$$

que é diferente de zero. Por outro lado, suponhamos que u é sufixo de y então,

$$(x^{-1}y)(u^{-1}v) = x^{-1}wv$$

que é diferente de zero.

Para terminar, determinemos uma descrição explicita do produto $(x^{-1}y)(u^{-1}v)$ quando este é diferente de zero. Usando os cálculos anteriores, sabemos que se $u = wy$, então,

$$(x^{-1}y)(u^{-1}v) = (wx)^{-1}v$$

e se $y = wu$ então,

$$(x^{-1}y)(u^{-1}v) = x^{-1}wv.$$

Facilmente se verifica que o produto tratado neste lema engloba estes dois casos e mais nenhum. □

A descrição anterior do produto conduz-nos a uma representação natural dos monoides policíclicos. Para $n \geq 2$, o monoide P_n é isomorfo ao conjunto $\Sigma^* \times \Sigma^* \cup \{0\}$ com a seguinte multiplicação:

$$(x,y)(u,v) = \begin{cases} ((uy^{-1})x,\ (yu^{-1})v) & \text{caso } \Sigma^* y \cap \Sigma^* v \neq \emptyset \\ 0 & \text{caso contrário.} \end{cases}$$

O elemento 0 é definido para funcionar como um zero.

O monoide P_1 é isomorfo a $\Sigma^* \cap \Sigma^*$ em que Σ contém exactamente um elemento com a multiplicação anterior, exceptuando a omissão do zero. Observando o isomorfismo entre o monoide livre, num alfabeto com apenas uma letra, e os inteiros com a adição, o monoide bicíclico é então isomorfo a um conjunto $\mathbb{N} \times \mathbb{N}$ com o produto:

$$(a, b)(c, d) = ((c \dot{-} b) + a,\ (b \dot{-} c) + d)$$

que é o produto definido no Capítulo 2.

Determinemos agora algumas propriedades importantes dos monoides policíclicos usando a representação dos seus elementos por pares ordenados.

Teorema 4.4. *Os monoides policíclicos são semigrupo inversos, combinatoriais, 0-bisimples, 0-E-unitários.*

Demonstração. Começamos por mostrar que os monoides policíclicos são inversos. Para o fazer, temos que caracterizar os idempotentes. Suponhamos que $(u, v)^2 = (u, v)$, então, $\Sigma^* v \cap \Sigma^* u \neq \emptyset$ e $u = (uv^{-1})u$ e $v = (vu^{-1})v$, logo, $u = v$. Facilmente se verifica que cada elemento da forma (u, u) é um idempotente.

Mostraremos seguidamente que os idempotentes comutam.
É claro que, $(u, u)(v, v) = 0$ precisamente quando $(v, v)(u, u) = 0$. Suponhamos então que $(u, u)(v, v)$ é diferente de zero, assim, u é um sufixo de v ou vice-versa, logo,

$$(u, u)(v, v) = ((vu^{-1})u,\ (uv^{-1})v) \quad \text{e} \quad (v, v)(u, u) = ((uv^{-1})v, (vu^{-1})u).$$

É imediato do Lema 4.2(3) que estes dois produtos são iguais e são idempotentes.

Note-se que $(u, v)(v, w) = (u, w)$, e portanto, $(u, v)(v, u)(u, v) = (u, v)$. Logo, os monoides policíclicos são inversos e $(u, v)^{-1} = (u, v)$. A ordem natural parcial tem uma caracterização simples. Suponhamos que $(u, v) \leq (x, y)$. Então, $(u, v) = (x, y)(v, v)$. Assim, $\Sigma^* y \cap \Sigma^* v$ é diferente do vazio e $u = (vy^{-1})x$ e $v = (yv^{-1})v$. Logo, y é um sufixo de v e x é um sufixo de u. Em particular, $(u, v) = (vy^{-1})(x, y)$. Assim, $(u, v) = p(x, y) = (px, py)$, para algum $p \in \Sigma^*$. Reciprocamente, se $(u, v) = p(x, y)$, para algum $p \in \Sigma^*$, então verificamos facilmente que $(u, v) \leq (x, y)$.

Para mostrar que o semigrupo é combinatorial, supomos que $(u, v)\mathcal{H}(x, y)$. Então, dos resultados anteriores obtemos $u = x$ e $v = y$.

Para mostrar que o semigrupo é 0-simples, consideramos (u, u) e (v, v) dois

elementos idempotentes diferentes de zero. Então,

$$(v,v) = (u,v)^{-1}(u,v) \quad \text{e} \quad (u,u) = (u,v)(u,v)^{-1}$$

e portanto $(u,u)\mathcal{D}(v,v)$.

Finalmente, para mostrar que o semigrupo é 0-E-unitário supomos que $(u,u) \leq (x,y)$. Então, $(u,u) = p(x,y)$, para algum $p \in \Sigma^*$. Logo, $x = y$, e portanto (x,y) é um idempotente. □

Uma propriedade fundamental dos monoides policíclicos, quando $n \geq 2$, é a seguinte:

Teorema 4.5. *Para todo $n \geq 2$, o monoide policíclico sobre n geradores é livre de congruências.*

Demonstração. Do Teorema 4.4 sabemos que P_n é 0-bisimples e portanto 0-simples. Assim, P_n não tem ideais para além dos triviais. Seja ρ uma qualquer congruência não-universal em P_n então, 0ρ é um ideal de P_n. Logo, $0\rho = \{0\}$ ou $0\rho = P_n$. Se ρ for a congruência não-universal $0\rho = \{0\}$. Suponhamos que ρ não é a congruência diagonal. Então, podemos encontrar um par de elementos distinto ρ-relacionados (x,y) e (x',y') tal que o comprimento

$$|x| + |y| + |x'| + |y'|$$

seja mínimo. Podemos assumir, sem perda de generalidade, que $x \neq 1$; isto porque pelo menos uma das variáveis x, y, x', y' deve ser não-vazia, caso contrário $(x,y) = (x',y')$, o que contradiz a nossa escolha de elementos. Mas então esta variável pode ser assumida como x, ou fazendo uma troca entre (x,y) e (x',y') ou observando que também se verifica $(x,y)\ \rho\ (x',y')$. Então, $x \in \Sigma^* a$ para alguma letra a, e portanto, $x = ua$ para alguma variável u.

Provaremos agora que $x' \neq \Sigma^* a$. Suponhamos que por absurdo que $x' = va$, para alguma variável v. Então

$$(1,a)(x,y)\ \rho\ (1,a)(x',y')$$

E portanto $(u,y)\ \rho\ (v,y')$. É claro que

$$|u| + |y| + |v| + |y'| < |x| + |y| + |x'| + |y'|.$$

Pela minimalidade isto implica que $(u,y) = (v,y')$, do qual podemos deduzir que $(x,y) = (x',y')$, uma contradição. Logo, x' nunca pode terminar com um a.

Existem agora duas possibilidades: ou $x' \in \Sigma^* b$ com $b \neq a$, possível porque $n \geq 2$, ou $x' = 1$. Suponhamos que $x' = vb$, então,

$$(1, b)(x, y) \ \rho \ (1, b)(x', y').$$

Temos $(1, b)(x, y) = 0$, visto que $(1, b)(x', y') = (v, y') \neq 0$, o que contradiz o facto de que $0\rho = \{0\}$. Logo, tem que se verificar $x' = 1$. Seja b uma qualquer letra tal que $b \neq a$. Então,

$$(1, b)(x, y) \ \rho \ (1, b)(1, y').$$

Contudo, $(1, b)(x, y) = 0$ visto que $(1, b)(1, y') = (1, by') \neq 0$. Temos mais uma vez uma contradição. O erro está no facto de termos assumido que ρ não é uma congruência diagonal.

□

Uma consequência do resultado anterior é que o semigrupo inverso obtido do conjunto de Cantor no início deste capítulo é mesmo isomorfo a P_2.

No resultado seguinte, provaremos que P_2 contém cópias de todos os monóides policíclicos em conjuntos numeráveis. Consideremos

$$P_2 = \langle p, q, p^{-1}, q^{-1} : pp^{-1} = 1 = qq^{-1}, pq^{-1} = 0 = qp^{-1} \rangle.$$

Proposição 4.6. *P_n está incluído em P_2 para todo $n \geq 2$, incluindo o caso em que $n = \infty$.*

Demonstração. Comecemos com alguns resultados preliminares. Fazendo $p_i = pq^i$ com $i \in \mathbb{N}$, então,

$$p_i p_i^{-1} = (pq^i)(pq^i)^{-1} = pq^i q^{-i} p^{-1} = 1.$$

Consideremos agora $p_i p_j^{-1}$ com $i \neq j$. É claro que, $p_i p_j^{-1} = pq^i q^{-i} p^{-1}$. Suponhamos que $j > i$. Então $j = i + k$, para algum $k > 0$, e portanto, $q^i q^{-j} = q^{-k}$. Logo $p_i p_j^{-1} = 0$. De forma análoga, quando $j < i$ então $p_i p_j^{-1} = 0$.

Seja $n \geq 2$ um número natural. Construiremos um semigrupo inverso de P_2 isomorfo a P_n. Definindo o subconjunto $\{p_{n,i} : 1 \leq i \leq n\}$ de P_2 da seguinte forma:

$$p_{n,i} = \begin{cases} pq^{i-1} & \text{com } i = 1, \ldots, n-1 \\ q^{n-1} & \text{com } i = n. \end{cases}$$

Dos nossos cálculos preliminares, é claro que $p_{n,i} p_{n,i}^{-1} = 1$ e $p_{n,i} p_{n,j}^{-1} = 0$, caso $i \neq j$ e $i \neq n$. Facilmente verificamos que $p_{n,n} p_{n,n}^{-1} = 1$ e que para $i \neq n$ temos

$p_{n,i}p_{n,n}^{-1} = 0$. Logo o conjunto $\{p_{n,i} : 1 \leq i \leq n\}$ gera um submonóide inverso P'_n de P_2 que é uma imagem homomorfa não trivial de P_n. Contudo, para $n \geq 2$ o monoide P_n é uma livre de congruências pelo Teorema 4.5. Logo, P_n é isomorfo a P'_n.

Suponhamos agora que $n = \infty$. Então prova-se de modo semelhante, que o conjunto $\{p_n : i \in \mathbb{N}\}$ gera um submonóide inverso isomorfo a P_∞. □

Um estudo mais extenso dos monóides policíclicos incluindo embeddings dos monóides policíclicos nos anéis, embeddings dos monóides policíclicos em $I(\mathbb{N})$ e ainda uma construção de Girard pode encontrar-se em Lawson [26].

2 Outras generalizações do Monoide bicíclico

Nesta secção referiremos brevemente outras construções com base no monoide bicíclico indicando as respectivas referências bibliográficas.

Em 1958 Bruck provou que qualquer semigrupo S pode ser "embeded" num monoide simples (com ideais próprios). Para isso ele definiu as extensões de Bruck-Reilly do monoide S^1. Reilly, em 1965, mostrou que os ω-semigrupos bisimples são as extensões de Bruck-Reilly de grupos. Em 1968, Kočin generalizou esta construção às cadeias finitas de grupos, caracterizando os ω-semigrupos bisimples inversos. Mais tarde, em 1970, Munn definiu o termo Extensões de Bruck-Reilly e provou que as extensões de Bruck-Reilly dos monoides de Clifford são os semigrupos simples inversos com um tipo especial de semireticulado de idempotentes.

Em [2] podemos encontrar a seguinte definição:

Seja M um monoide com identidade 1_M e seja $\theta : M \to M$ um endomorfismo de M. No conjunto $\mathbb{N}_0 \times T \times \mathbb{N}_0$ (em que $\mathbb{N}_0$ representa o conjunto dos inteiros não negativos) definimos a seguinte operação binária

$$(m, a, n)(p, b, q) = (m - n + t, (a\theta^{t-n})(b\theta^{t-p}), q - p + t)$$

em que $t = \max\{n, p\}$, e θ^0 denota a aplicação identidade em M. O conjunto $\mathbb{N}_0 \times T \times \mathbb{N}_0$ com esta operação é um monoide com identidade $(0, 1_m, 0)$, que denotamos por $\mathrm{BR}(T, \theta)$ e chamamos a *extensão de Bruck-Reilly de M determinada por θ*. Esta construção é uma generalização das construções feitas por Bruck [3], Reilly [31] e Munn [29]. A construção de Bruck considera o caso especial em que θ aplica todos os elementos na identidade de M, onde a extensão obtida é um monoide simples, e é usada para provar que todo o semigrupo pode ser "embeded" num monoide simples.

Por outro lado, a construção de Reilly considera o caso em que o monoide é um grupo; o monoide obtido é um ω-semigrupo inverso bisimples e, reciprocamente, todo ω-semigrupo inverso bisimples é uma extensão de Bruck-Reilly do seu grupo de unidades. E por fim, Munn considera as extensões de Bruck-Reilly com respeito a endomorfismos que aplicam o monoide no seu grupo de unidades e assim dá um teorema de estrutura para uma classe especial de semigrupos inversos simples ([29]).

Fazemos agora uma breve referência a Celia L. Adair que em [1] descreve uma generalização dum semigrupo bicíclico, que é o semigrupo de isomorfismos entre ideais principais do semireticulado $c_w = \{\alpha_0 > \alpha_1 > \ldots > \alpha_n > \ldots\}$. Adair considera N como conjunto representante de todos os números (facilmente se mostra que o semigrupo bicíclico é isomorfo a $(N \times N, \cdot)$ com $(m,n) \cdot (p,q) = (m - n + \max\{n,p\}, q - p + \max\{n,p\})$), e a generalização do semigrupo bicíclico é descrita de tal modo que matrizes substituem os pontos de $(N \times N)$ e para os quais a imagem inversa máxima é o semigrupo bicíclico.

3 Considerações finais

Esta dissertação consiste num trabalho de recolha bibliográfica e síntese sobre o monoide bicíclico propriedades, subsemigrupos, e generalizações. Definimos assim o monoide bicíclico e apresentamos algumas propriedades notáveis do mesmo, fizemos a descrição de todos os subsemigrupos do monoide bicíclico que utilizamos para estabelecer diversas propriedades destes subsemigrupos. Estudamos apenas em detalhe uma generalização e referimos outras. Foram incluídos resultados recentes, nomeadamente sobre subsemigrupos.

Terminamos esta dissertação com a ideia de que ainda há muito trabalho por fazer, nomeadamente na investigação dos subsemigrupos do monoide bicíclico, procurando eventualmente ligações com a teoria dos subsemigrupos numéricos.

BIBLIOGRAFIA

[1] C. L. Adair, *A generalization of the bicyclic semigroup*, Semigroup Forum **21** (1980), 13–25.

[2] I. M. Araújo and N. Ruškuc, *Finite presentability of Bruck-Reilly extensions of groups*, J. Algebra **242** (2001), 20-30.

[3] R. H. Bruck, *A survery of binary systems*, Ergebnisse der Math., Neue Folge, Springer, Berlin **20** (1958).

[4] K. Byleen, J. Meakin and F. Pastijn, *The fundamental four-spiral semigroup*, J. Algebra **54** (1978), 6–26.

[5] C. M. Campbell, E. F. Robertson, N. Ruškuc and R. M. Thomas, Automatic semigroups, *Theoret. Comput. Sci.* **250** (2001), 365–391.

[6] L. Descalço and N. Ruškuc, *Subsemigroups of the bicyclic monoid*, Int. J. Algebra Comput. **15** (2005), 37–57.

[7] L. Descalço and N. Ruškuc, *Properties of the subsemigroups of the bicyclic monoid*, Accepted for publication.

[8] T. Ersova, *Inverse semigroups with certain types of lattices of inverse subsemigroups* (Russian), Ural. Gos. Univ. Mat. Zap. **7** (1969/1970), 62-76.

[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.2*; 2000, (`http://www.gap-system.org`).

[10] P. Goralcik, *One remarkable property of the bicyclic semigroup*, Commentat. Math. Univ. Carol. **12** (1971), 503-518.

[11] P. A. Grillet, *On the fundamental double four-spiral semigroup*, Bull. Belg. Math. Soc. Simon Stevin **3** (1996), 201–208.

[12] P. A. Grillet, *Semigroups, An Intruductuion to the Structure Theory*, Lousiana,Tulane University, 1995.

[13] M. Hoffmann, N. Ruškuc and R. M. Thomas, Automatic semigroups with subsemigroups of finite Rees index, *Internat. J. Algebra Comput.* **12** (2002), 463–476.

[14] M. Hoffmann and R. M. Thomas, Notions of automaticity in semigroups, *Semigroup Forum* **66** (2003), 337–367.

[15] K. H. Hoffmann, M. W. Mislove, All compact Hausdorff lambda models are degenerate, *Fundamenta Informatica* **22** (1995), 23-52.

[16] K. H. Hoffmann, M. W. Mislove, Principles underlying the degeneracy of topological models of the untyped lambda calculus, in *Semigroup theory and its applications* (eds K. H. Hofmann, M. W. Mislove), Cambridge University Press, Cambridge, (1996), 123-155.

[17] J. W. Hogan, *The α-bicyclic semigroup as a topological semigroup*, Semigroup Forum **28** (1984), 265–271.

[18] J. M. Howie, *Fundamentals of Semigroup Theory*, Oxford University Press, 1991.

[19] N. Jacobson, Some remarks on one-sided inverses, *Proceedings of the American Mathematical Society* **1** (1950), 352-355.

[20] P. R. Jones, *Distributive inverse semigroups*, J. London Math. Soc. **17**(2) (1978), 457-466.

[21] J. Justin and G. Pirillo, *Comments on the permutation property for semigroups*, Semigroup Forum **39** (1989), 109-112.

[22] J. Justin and G. Pirillo, *Some remarks on the permutation property for semigroups*, Europ. J. Combinatorics **11** (1990), 151-154.

[23] B. P. Kochin, *The structure of inverse ideal-simple ω-semigroups*, Vestnik Liningrad Univ. **23** (1968), 41-50.

[24] G. Lallement, *Semigroups and Combinatorial Applications*, John Wiley & Sons, 1979.

[25] G. Lallement, *On monoids presented by a single relation*, J. Algebra **32** (1974), 370–388.

[26] M. V. Lawson, *Inverse Semigroups*, World Scientific, 1998.

[27] S. O. Makanjuola and A. Umar, *On a certain subsemigroup of the bicyclic semigroup*, Comm. Algebra **25** (1997), 509–519.

[28] W.D.Munn, *Regular ω-semigroups*, Glasg. Math. J. **9** (1968), 46-66.

[29] W. D. Munn, *On simple inverse semigrups*, Semigroup Forum **1** (1970), 63-74.

[30] M. Nivat, J.-F.Perrot, Une Généralisation du monoïde bicyclique, *Comptes Rendus de l'Académie des sciences de Paris* **271** (1970), 824-827.

[31] N. R. Reilly, *Bisimple ω-semigroups*, Proc. Glasgow Math. Assoc. **7** (1966), 160-167.

[32] J. C. Rosales and P. A. García-Sánchez, *Finitely Generated Commutative Monoids*, Nova Science Pulishers, Commack NY,1999.

[33] N. Ruškuc, On large subsemigroups and finiteness conditions of semigroups, *Proc. London Math. Soc.* **76** (1998), 383–405.

[34] L. N. Shevrin, *The bicyclic semigroup is determined by its subsemigroup lattice*, Simon Stevin **67** (1993), 49–53.

[35] L. N. Shevrin and A. J. Ovsyannikov, *Semigroups and Their Subsemigroup Lattices*, Kluwer Academic Publishers, 1996.

[36] Vachuska, Colleen and Vachuska, Peter, *The bicyclic semigroup has S_4^**, Semigroup Forum **47** (1993), 133–134.